Microsoft Corporation
One Microsoft Way
Redmond, WA 98052-6399

Tel 425 882 8080
Fax 425 706 7329
www.microsoft.com

April 25, 2022

Uploaded to www.regulations.gov

With courtesy copies to CSF-SCRM-RFI@nist.gov

National Institute of Standards and Technology
United States Department of Commerce
100 Bureau Drive
Gaithersburg, MD 20899

Subject: Microsoft Comments on National Institute of Standards and Technology's Request for Information on Evaluating and Improving NIST Cybersecurity Resources: The Cybersecurity Framework and Cybersecurity Supply Chain Risk Management

References: Docket Number: 220210-0045

I. Introduction

Microsoft welcomes the opportunity to provide comments to the National Institute of Standards and Technology (NIST) regarding the Request for Information (RFI) on Evaluating and Improving NIST Cybersecurity Resources: The Cybersecurity Framework and Cybersecurity Supply Chain Risk Management. As a provider of technology products and services to more than one billion customers in the United States and worldwide, Microsoft is constantly innovating and investing in developing, maturing, and promoting cybersecurity best practices both internally and externally.

Microsoft supports NIST's commitment to updating and strengthening use of the *Framework for Improving Critical Infrastructure Cybersecurity* ("Framework"). We are also eager to contribute to the National Initiative for Improving Cybersecurity in Supply Chains (NIICS). NIST's efforts to integrate supply chain security more comprehensively into the Framework while also driving broader adoption and use of supply chain risk management tools, technologies, and guidance demonstrate the complexity and importance of addressing growing supply chain threats.

Because of NIST's collaborative approach to welcoming input and feedback from government, industry, and civil society partners, Microsoft has had the opportunity to contribute to the development of the Framework, including Versions 1.0 and 1.1. We encourage NIST to continue leveraging multi-stakeholder processes, including previous and new models of engagement, throughout the Framework update process and instantiation of NIICS. We reiterate that Microsoft has been an enthusiastic supporter of the Framework and, through this submission, confirm our continued commitment to leveraging NIST resources and partnering on their development.

We have organized our comments in response to NIST's RFI into four substantive sections. Section II offers high-level recommendations on strengthening cybersecurity and supply chain risk management through the Framework, NIICS, and other NIST cybersecurity and risk management resources. Section III discusses our support for leveraging a multi-stakeholder approach to the Framework update process. Section IV details our answers to specific questions in the RFI. Finally, Section V offers our recommendations for cybersecurity supply chain risk management, including input on how to ensure that the Framework adequately addresses cybersecurity supply chain risk management.

II. Framework 2.0 Revision and NIICS: An Opportunity to Strengthen Cybersecurity and Supply Chain Risk Management

Since the Framework was last updated four years ago, connectivity and risk have continued to grow, driving the development of dozens of cybersecurity resources and regulations.[1] Yet a fundamental challenge of cybersecurity risk management has remained constant: dynamic technology and threats demand ongoing innovation in security practices. This amalgamation of trends and steady challenges has created enormous complexity, which is primed to increase further as regulation continues to multiply and risk splintering globally and across sectors.

Despite this environment, the Framework has served as an exceptionally useful resource in part because its organization and flexibility have allowed users to adapt it to their needs, including by integrating complementary standards or guidance and leveraging evolving security practices. However, the proliferation of cybersecurity resources and regulation – and associated certification, compliance, or capability assessments, which often tax assessment-fatigued security professionals – is testing its capacity to stretch in a way that continues to add value versus complexity. In addition, demands for more robust measurement and compliance pressure the Framework to stretch in new ways.

The Framework 2.0 revision can respond to these and other challenges as part of a broader NIST and U.S. government effort to focus and align resources and ensure security compliance is

[1] The RFI acknowledges that much has changed in the cybersecurity landscape regarding threats, capabilities, technologies, education, workforce, and the availability of resources to help organizations manage risk.

grounded in robust risk management practices. We offer the following high-level recommendations to inform the revision process: 1) drive cohesion, interoperability, and simplicity, not just at the structural level of NIST's resources but also in how they are implemented in practice; 2) strengthen awareness and understanding across multiple audiences, and 3) invest in future proofing.

Drive cohesion, interoperability, and simplicity

Microsoft commends NIST's focus on evaluating and improving the Framework along with other frameworks and risk management resources. We believe this approach sets the stage for a comprehensive examination of NIST's resources and how they work together to help strengthen cybersecurity risk management for an organization. While NIST has developed numerous frameworks and guidance documents to support practitioners and earned wide recognition for its cybersecurity standards and best practices expertise, many organizations are overwhelmed by the breadth and depth of NIST's resources. Individual resources may be extensive or complex, and how to use complementary resources concurrently but efficiently may be unclear.

A simplified, interoperable suite of NIST cybersecurity and risk management resources, which may require structural changes to resources as well as procedural changes to development processes, would increase accessibility and reduce uncertainty. In addition, cohesion and alignment of cybersecurity and risk management resources with the Framework would empower cybersecurity practitioners to use NIST resources holistically to strengthen cybersecurity risk management programs. It may also help users clarify how they can leverage the Framework and other NIST resources to meet or demonstrate conformance with other cybersecurity requirements, grounding compliance exercises in robust risk management processes.

One area in which there's an opportunity to better integrate, simplify, and ensure cohesion across resources is cybersecurity supply chain risk management. As further discussed below, we support NIST's intention to ensure that the Framework sufficiently addresses supply chain security considerations and practices. Cybersecurity supply chain risk management is a cross-cutting issue, and we recommend that it is integrated across the Framework's Categories. We encourage the use of NIST Special Publication (SP) 800-218, the Secure Software Development Framework (SSDF), as well as recognition of the need to incorporate practices into the Framework or issue guidance on how to use the SSDF along with the Framework. [2] We also

[2] In our review, we identified several gaps: 1) the Framework focuses on the role of a consumer, whereas SSDF addresses the role of a supplier; 2) the Framework seems to incompletely cover choosing, acquiring, and building the necessary tools to implement processes in the Asset Management Category; and 3) the Framework seems to not cover root cause analysis and improving underlying processes to avoid the root causes reoccurring in the Respond and Recover Functions.

encourage NIST to address the intimidating nature of NIST SP 800-161 by exploring how to incorporate what's necessary into the Framework or other publications, retain valuable components, and remove areas of overlap.

Strengthen awareness and understanding across multiple audiences

NIST's effort to evaluate and improve cybersecurity resources presents an opportunity to likewise review how content is delivered, promoted, and accessed. While NIST's many thorough, detailed resources reflect its expertise as well as the complexity of comprehensive cybersecurity practices, some practitioners could struggle to consume and apply them, therefore hampering use and impact. NIST could explore opportunities to deliver cybersecurity risk management resources in various formats to cater to different audiences with varying levels of expertise. Succinct implementation guidance could explain how the SSDF could be used alongside the Framework. Additional investment in showcasing on NIST's website and otherwise the vast number and relevance of its cybersecurity and risk management resources could also increase awareness and understanding of how they can be used effectively, especially among targeted stakeholders.

Invest in future proofing

The Framework must remain flexible, agile, and responsive to fast-paced technologies and the expanding attack surface, which shows no signs of slowing down. As more organizations seek to harness technologies and architectures such as cloud computing, machine learning (ML), artificial intelligence, internet of things (IoT), Industrial internet of things (IIoT), 5G, and Zero Trust, approaches to cybersecurity risk management will continue to evolve, likely at a cadence sooner than four or five years from now. What structures or processes can help ensure the Framework likewise continues to evolve along with the broader ecosystem? These and other complex questions require considerable deliberation through an iterative and transparent multi-stakeholder approach.

III. Use an iterative and transparent multi-stakeholder process to develop Framework v2.0 and NIICS

Microsoft applauds NIST's continuous engagement and collaboration with industry, academia, and government stakeholders to develop cybersecurity standards, guidelines, best practices, and other resources to improve the overall security of the domestic and international ecosystem. Microsoft is highly supportive of the stakeholder engagement model NIST used during the Framework v1 and v1.1 development processes and enthusiastically recommends NIST use a similar approach to update the Framework v2 and NIICS. Specifically, Microsoft recommends that NIST allow for numerous opportunities for feedback and dialogue through various public comment processes, in-person and virtual meetings, workshops, and outreach

and consultation with domestic and international stakeholders. Iterative processes that allow for discussion foster cross-sector communication, shared learning, and consensus-building among stakeholders.

In addition, NIST could consider leveraging working groups comprised of diverse stakeholders to address challenging RFI questions or NIICS goals. In our experience, in contributing to multiple industry efforts to provide NIST feedback on this RFI, various understandable but in some cases divergent perspectives were elicited in discussing complex topics like cybersecurity supply chain risk management. Working groups could allow for more substantive and technical conversations and support NIST in discussing comments received in response to this RFI and formulating recommendations. In addition, working groups could support NIST in exploring ways to consolidate and align resources. While working groups could not fully represent or make decisions on behalf of industry, nor infringe on NIST's decision-making role, they could offer a regular sounding board and set of resources and expertise committed to supporting positive outcomes for the ecosystem.

IV. Responses to Specific RFI Questions

In addition to our general comments above, Microsoft appreciates the opportunity to share the following feedback, presented in alignment with specific questions asked in the RFI:

Use of the NIST Cybersecurity Framework

1. The usefulness of the NIST Cybersecurity Framework for aiding organizations in organizing cybersecurity efforts via the five functions in the Framework and actively managing risks using those five functions. In addition, the Current benefits of using the NIST Cybersecurity Framework. Are communications improved within and between organizations and entities (e.g., supply chain partners, customers, or insurers)? Does the Framework allow for better assessment of risks, more effective management of risks, and increase in the number of potential ways to manage risks? What might be relevant metrics for improvements to cybersecurity as a result of the implementation of the Framework?

Since 2014, Microsoft has used the Framework to assess the company's security capability. Microsoft has integrated the Framework into our enterprise risk management program to influence our security risk culture and inform how we communicate security capability maturity across our senior management and Board of Directors. Microsoft regularly conducts assessments through the implementation of the Framework, covering a broad mix of customer-

facing and internal infrastructure services across the enterprise. These assessments are the foundation for comprehensive, internal discussions that extend from operational levels to senior leadership and the Board of Directors about security capability and continuous improvement efforts.

As an external best practice that applies across our key services and different risk management roles, the Framework enables conversations with diverse expertise and focus areas across practitioners and management teams. One of the most prominent benefits of the Framework is that it serves as a vehicle to enable such discussions about Microsoft's security profile across organizational silos and subcultures and to bring leaders together to talk about critical capability, aspirations, and future investments in a risk-based format. The Framework provides us with a common language to consistently discuss security across our offerings, simplifying communications and enabling senior leaders to actively engage in discussions about security activities and new investments in risk management processes or security capabilities. Microsoft actively uses the Framework concept of a Target Profile to allow for a focused measure of security capability, discuss priorities, and track gaps and progress over time, supporting a continuous improvement culture.

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 practical 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 align their concerns, tolerance, and resources—and 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.

The Framework benefits security by promoting interoperability and strong alignment with global best practices and reference points, including ISO/IEC 27103 and ISO/IEC 27001. Microsoft uses the Framework to develop a unified view of security capability using an external standard and reconcile multiple security approaches and compliance requirements. While maintaining alignment with the Framework structure, Microsoft appreciates the Framework's flexibility to integrate with various informative references (e.g., ISO/IEC 27001) and global approaches (i.e., ISO/IEC 27103). Because of its flexibility and interoperability, Microsoft has adopted and benefited from the Framework to limit operational disruption and minimize duplication of efforts.

2. Challenges that may prevent organizations from using the NIST Cybersecurity Framework or using it more easily or extensively (e.g., resource considerations, information sharing restrictions, organizational factors, workforce gaps, or complexity)

As discussed in the context of the following section, Microsoft has addressed challenges using the Framework as we've iterated on and improved our internal assessments; however, no challenge has prevented us from using the Framework. Therefore, we raise here challenges that we understand may prevent partners and other organizations from using the Framework as well as related recommendations, building on the themes we offered above in Section II.

i. Improve content delivery, accessibility, and promotion of the Framework and other NIST resources

The volume of NIST resources offers both an opportunity and a challenge. On NIST's website, there is likely to be a resource responsive to questions a practitioner might ask, but practitioners may struggle to 1) find resources efficiently; 2) understand all the resources available; and 3) how resources relate to each other to manage risk. For example, for those new to the Framework and unaware of the NIST's ecosystem of resources, the path from the Framework landing page[3] to the SSDF, the Privacy Framework, or even the version of the Framework targeting small businesses (*NISTIR 7621 – Small Business Information Security: The Fundamentals*) may not be intuitive.

In addition, the Cybersecurity Framework: International Use landing page[4] has minimal content to provide context to international partners on the Framework or successful adaptations. As NIST focuses on increasing international adoption of the Framework, it should have a user-friendly, informative, and visually appealing landing page describing its global adaptation of the Framework, alignment with international best practices, and Framework translations.

A landing page that serves as a one-stop-shop for NIST's risk management resources could allow for easy navigation to the Framework, and related topics, whether sectors, attack vectors, or other risk management frameworks, and cater to different audiences, i.e., small business vs. international users. For example, NIST's Cybersecurity for IoT Program landing page[5] displays information for different audiences such as manufacturers, federal agencies, and consumers. Further, a cohesive information architecture would better clarify the relationship between NIST resources. For example, Framework > implementation guidance by industry or technology> specific controls, etc. This recommendation is not exhaustive and only stated to illustrate the need for streamlined and navigable online resources to enhance the overall user experience, especially for those less familiar with NIST and the Framework. A good starting point to

[3] https://www.nist.gov/cyberframework
[4] https://www.nist.gov/video/cybersecurity-framework-international-use
[5] https://www.nist.gov/itl/applied-cybersecurity/nist-cybersecurity-iot-program

increasing awareness of NIST resources is to ensure that practitioners can quickly and easily access these resources, ideally in a way that demonstrates how they relate to each other.

ii. Explore alternative formats for content delivery

Some practitioners could find detailed NIST publications difficult to consume due to time and resource constraints or varying experience levels. NIST could therefore explore opportunities to deliver the Framework's contents in various formats to cater to different audiences with varying levels of expertise and time constraints. For example, NIST could develop Framework 101 fact sheets, Framework two-pager user guides, short implementation guides, or brief tutorial videos. These resources would likely be particularly worthwhile to develop if coupled with easily navigable landing pages and coordinated efforts to drive potential user awareness.

3. Any features of the NIST Cybersecurity Framework that should be changed, added or removed. These might include additions or modifications of: Functions, Categories, or Subcategories; Tiers; Profile Templates; references to standards, frameworks, models, and guidelines; guidance on how to use the Cybersecurity Framework; or references to critical infrastructure versus the Framework's broader use

i. Revisit Functions of the Framework as well as other resources

The Framework's five existing Functions, as reflected in Versions 1.0 and 1.1, provide an effective way to organize a cybersecurity risk management program and frame activities so that they can be accessible to multiple audiences (i.e., their overall goals can be easily understood). However, we encourage NIST to consider whether and how to add an additional Govern Function. While we see potential benefits to doing so as described below, we also note potential drawbacks, such as alignment with international resources (e.g., ISO/IEC standards and technical reports) and references (e.g., agreements that describe the five Functions as a frame for cybersecurity best practices) to the Framework.

Microsoft encourages NIST to evaluate whether the Governance Category is sufficient in addressing an organization's overall security risk management or if there would be additional value to a Govern Function given ecosystem trends and opportunities to align with other resources. Cybersecurity governance has become increasingly important due to the increased sophistication of threats and exploits, the proliferation of technologies such as cloud computing and IoT, the managing of third-party services, and other supply chain complexities. In addition, increased cybersecurity regulation of critical infrastructure sectors requires cybersecurity governance teams to effectively manage strategic alignment, risk management compliance, and value delivery. In addition, NIST has included the Govern Function in the NIST Privacy Framework and AI Risk Management Frameworks. For example, the Privacy Framework states that the Govern Function is "similarly foundational but focuses on organizational-level activities such as establishing organizational privacy values and policies, identifying legal/regulatory

requirements, and understanding organizational risk tolerance that enables an organization to focus and prioritize its efforts, consistent with its risk management strategy and business needs." Meanwhile, the AI Risk Management Framework states that the Govern Function "is a cross-cutting function that is infused throughout and informs the other functions of the process. Aspects of Govern, especially those related to compliance or evaluation, should be integrated into each of the other functions." These issues are relevant to cybersecurity and could bolster the Framework. Note that opportunities to drive cohesion and alignment between the Cybersecurity Framework, Privacy Framework, and AI Risk Management Framework are further discussed below in Section IV, sub-section 5.

ii. Update the PR.DS (Protect - Data Security), PR.PT (Protect - Protective Technology) and RC (Recovery) Categories

Microsoft recommends several updates to the PR.DS (Protect Data Security), PR.PT [Protect Protective Technology), and RC (Recovery) Categories. As currently scoped, PR.DS is insufficient to protect against threats today, especially to critical infrastructure; specifically, PR.DS-1 covers data-at-rest and PR.DS-2 covers data-in-transit, but the third leg of data-in-use is missing; we recommend adding a Subcategory. Today, the confidential computing industry and the Confidential Computing Consortium[6] address this third leg with many tools and solutions.

PR.DS-6 and PR.DS-8 mentions "integrity checking," which often implies on-device checking, and is weaker than "remote attestation," which provides a much stronger level of verification. Microsoft recommends either updating both to mention remote attestation or adding another Subcategory that refers to remote attestation.

PR.PT could also be updated, either by adding to existing Subcategory language or creating new Subcategories, to incorporate the latest approaches, including practices recommended by NIST in other cybersecurity publications. For instance, this Category could emphasize the importance of using "immutable hardware root of trust" (in the language of NISTIR 8259 section 3.4).

Finally, the RC Category could incorporate best practices that allow for the ability to recover a given system from a bad state. NISTIR 8259 section 4.2.4 and NISTIR 8259A both discuss software updates. Existing standards, such as the Trusted Platform Module Library[7] and Device Identifier Composition Engine[8] from the Trusted Computing Group (TCG),[9] support verifying the recovery of a compromised system if hardware roots of trust are not compromised. Further guidance on recovering firmware and critical data of compromised devices (and their components) reside in NIST SP 800-193. Such approaches to recovery and verification when

[6] https://confidentialcomputing.io/

[7] https://trustedcomputinggroup.org/resource/tpm-library-specification/
[8] https://trustedcomputinggroup.org/resource/hardware-requirements-for-a-device-identifier-composition-engine/
[9] https://www.trustedcomputinggroup.org/.

integrity is compromised are critical, especially for infrastructure where expensive physical systems make hardware replacement impractical.

iii. Integrate ID.SC (Supply Chain Risk Management) Category

We support NIST's interest in exploring how to further integrate supply chain risk management into the Framework. We recommend a full review of the Framework to determine what supply chain risk management practices are appropriate across Functions. Please see our response in Section 5 for further recommendations on the Supply Chain Risk Management Category (ID.SC).

iv. Clarify Subcategories to foster more straightforward implementation and close security gaps

Practitioners at times struggle to understand what each Subcategory means for their specific context. The challenge lies in how to identify and define the specific processes, functions, or controls each Subcategory is meant to encompass, as well as what level of maturity corresponds to which Tier in the Framework. Cybersecurity practitioners have expressed a need for more guidance on how to assess each subcategory with this in mind.

The program office that manages our regular Framework assessments at Microsoft has developed a set of questions to give practitioners practical advice on scoping and assessing the Subcategories to alleviate this problem. Along with the set of questions, Microsoft has created rating guidance, which suggests answers that may correspond to a Tier within the Framework. In addition, Microsoft has found that these questions reduce subjectivity in self-assessments. For example, for *DE.CM.1: The network is monitored to detect potential cybersecurity events*, Microsoft's questions include:

- Does the team have a dedicated response team for alerts generated by the network monitoring system?
- Are the policies and procedures for the continuous network monitoring process documented?
- Does the service employ detection capabilities for behavioral analytics, anomaly detection, IDS, and exceeding general performance thresholds? (i.e., Expected data flows and expected bandwidth to help monitor any anomalous activity.)
- How often are the detection values/rules for alerting reviewed?

For each question, answers corresponding to different Tiers are provided to support the assessor in considering the manner in which a process or control is implemented, along with an explanation of what level of maturity of implementation corresponds to which Framework Tier. Microsoft recommends that NIST develop similar guidance for Subcategories.

v. Clarify Framework Implementation Tiers ("Tiers") and Framework Profile ("Profile") Components

NIST should consider updating the Tier definitions to make them easier to implement and reflect continuous improvement within each Tier. Framework v1.1 describes the Current Profile

as cybersecurity outcomes that are currently being achieved and the Target Profile as the outcomes needed to achieve the desired cybersecurity risk management goals. While the definitions above are accurate, they are not immediately apparent to practitioners implementing the Framework. One possible way to simplify the definitions above is by modifying the current definitions to explicitly state that the Current Profile and Target Profile are designated implementation Tier levels. For example, the Target Profile could be explained as *the Tier that reflects* the *state of* outcomes needed to achieve the desired cybersecurity risk management goals. At the same time, the Current Profile could be explained as the *Tier that reflects the state of* cybersecurity outcomes that are currently being achieved.

Furthermore, there needs to be more guidance for an organization to assess whether it is meeting Tier definitions**.** Framework v1.1 describes the state of an organization's risk management practices for its risk management process, integrated risk management program, and external participation for each Tier. These descriptions are broad and require further clarification. For example, suppose an organization sets its Current Profile at 2 and its Target profile at 3 for all the Framework Categories. What key markers can it use to ensure that its cybersecurity outcomes meet the Tier level expectations? To strengthen use of the Tiers in a Framework v2.0, we recommend NIST consider issuing guidance to assist organizations in gaining a solid understanding of and confidence in what it takes to meet their Tier determinations.

Lastly, the current Tier levels 1-4 do not allow organizations to account for continuous improvement over time within each Tier. For example, if a product team has attained a Tier 2 for three consecutive years but has continuously improved over those three years, how does the Framework account for those important incremental changes? Microsoft recommends that NIST consider how to allow for ratings that can show continuous year-to-year improvement. One possible solution may be to create low, moderate, or high sub-levels within Tiers, accompanied by guidance on attaining them.

4. Additional ways in which NIST could improve the Cybersecurity Framework or make it more useful.

i. Address cloud security in the Framework or supporting resources, such as a cloud profile

Many critical infrastructure partners are transforming their businesses by leveraging cloud computing technology. Microsoft works with critical infrastructure providers worldwide and sees the unique challenges they face in digitally transforming, including in understanding, and managing cloud security. In addition to strengthening the security of cloud deployments, heavily regulated critical infrastructure entities need assurance that security practices map to regulatory standards.

Common challenges faced by our critical infrastructure customers or service partners include:

- Need for security best practices guidance to ensure a secure deployment of cloud services and their workload and to improve the security posture of existing cloud deployments to prioritize top risks and mitigations;
- Need for guidance to support evaluations of cloud services' security features/capabilities before onboarding/approving a service into the cloud service catalog; and
- Need for support in meeting compliance requirements in highly regulated industries, including by ensuring that their service configurations meet the security specifications defined in NIST, Center for Internet Security (CIS), Payment Card Industry (PCI), or other frameworks, control sets, or security standards.

We frequently hear from cloud customers that, beyond the Cloud Security Alliance (CSA) Cloud Control Matrix, there aren't many resources to support operational security of cloud deployments. Microsoft has developed the Azure Security Benchmark (AZB v3) and other resources to fill this gap for our customers. AZB v3 helps Azure users plan their cloud deployments by reviewing the documentation for the enterprise controls and service-specific baselines to design their control framework and how it maps to NIST, CIS, or PCI guidance or standards.

Microsoft understands that the Framework needs to remain technology-agnostic to retain flexibility and relevance for audiences using different technologies. However, given the widespread use of cloud computing technology, we recommend that NIST uses a multi-stakeholder approach to develop a cloud profile. We note that the Cyber Risk Institute recently completed a "Cloud Profile," a cloud extension of the CRI Profile version 1.2, to provide "guidance to financial institutions and CSPs on commonly understood responsibilities related to cloud deployment…" We also understand that other sectors are considering the development of such a profile and encourage consideration of the value that a cross-sector cloud profile might have to support consistency across sectoral efforts. A cloud profile would also provide all organizations with guidance on addressing cloud security risks holistically while using the Framework.

In addition, NIST should consider how to amplify awareness and understanding of how to use sectoral and cloud profiles that leverage the Framework. While NIST provides links to such resources on both the "Critical Infrastructure" and "Example Profiles" tabs of the Risk Management Resources page, there's minimal context for understanding their purpose or supporting use. The Coalition to Reduce Cyber Risk (CR2) has developed a white paper, *Seamless Security*,[10] to describe how international, national, and sectoral frameworks can leverage common baselines to enable consistency and interoperability, but we continue to see opportunities to strengthen awareness and understanding of the purpose of profiles and how they can be used.

[10] https://www.crx2.org/seamless-security-white-paper-press-release

Furthermore, Microsoft would welcome the opportunity to create an Azure Security Benchmark Informative Reference through the NIST National Online Informative References (OLIR) Program.

5. Relationship of the NIST Cybersecurity Framework to Other Risk Management Resources: Suggestions for improving alignment or integration of the Cybersecurity Framework with other NIST risk management resources. As part of the response, please indicate benefits and challenges of using these resources alone or in conjunction with the Cybersecurity Framework

Silos and cross-organizational communication and collaboration are issues that plague many private and public sector organizations. Even organizations that excel in this area understand that doing so requires continuous maintenance and improvement. However, just as the Framework can be used as a communication tool to drive coherence in cybersecurity risk management conversations across an organization's silos, so too can NIST's suite of risk management frameworks and resources drive critical communication and coordination across broader organizational efforts. To do so most effectively, these frameworks and resources must not only be structured in a consistent way but also interoperable when implemented.

Microsoft appreciates NIST's efforts to respond to the complex and rapidly changing technology landscape by developing numerous risk management and cybersecurity resources, such as the NIST Privacy Framework, AI Risk Management Framework (RMF), NIST SP 800-161, NISTIR 8259, and NISTIR 8374. Microsoft commends the way NIST leveraged the Framework structure to facilitate developing and using the Privacy Framework, AI RMF, and SSDF. That consistent structure enables practitioners and leaders to quickly understand how to use the frameworks, coordinate with others across their domains, and have appropriate flexibility in risk- and outcome-based approaches.

However, further alignment of the frameworks would support more coherent cross-domain conversations and more interoperable use. Structurally, Function-level alignment, either across the frameworks or in an organizing construct that applies to each of them, could be useful. NIST could consider the feasibility and value of adding new Functions to align the Cybersecurity Framework with its other frameworks. For example, Governance is a Category in the Cybersecurity Framework but at the Function level in the Privacy Framework and draft AI RMF. That structural difference also reverberates further; GV.RM-P is Risk Management Strategy under the Governance function of the Privacy Framework, but in the Cybersecurity Framework v1.1, Risk Management Strategy falls under the Identify Function and is separate from Governance. Another possible option could be to keep the Cybersecurity Framework Functions static and avoid duplicating Functions in other frameworks, instead including only functions unique to those domains.

Beyond structural alignment, we believe there are more significant gaps in helping organizations recognize how to implement the frameworks in a coordinated and non-duplicative manner. Ultimately, NIST has an opportunity to better integrate cybersecurity, privacy, and AI risk management convergence activities into complementary frameworks and supplement with guidance on how to use them together. While the Privacy Framework recognized critical intersections between both domains, recent trends continue to reinforce the importance of coordinating across cybersecurity and privacy risk management activities; for instance, more and more ransomware attacks include a data exfiltration component, directly linking them to privacy concerns. Likewise, with the ongoing development of the AI RMF, Microsoft recommends that NIST should: (1) drive alignment between the Cybersecurity Framework and supply chain work with that of the AI RMF and (2) develop taxonomies and methods to help organizations inventory AI systems and machine learning (ML) models for the purposes of risk management efforts across domains. We recognize that different NIST teams and divisions are likely responsible for different subject areas and the development of cybersecurity, privacy, and other risk management resources and encourage collaboration processes that help ensure cohesion.

In addition, Microsoft recommends that NIST include Zero Trust efforts and taxonomy to stay ahead of the curve of Zero Trust implementations. Practitioners need to understand how Zero Trust principles may change their control-level decisions and move from 'checklist' security compliance to holistic modalities that are more agile within the five functional areas. NIST should consider referencing NIST SP 800-207: Zero Trust Architecture and more substantially integrating the principles/tenets of Zero Trust into the Categories and Sub-categories that support the five functional areas. Similarly, NIST should integrate other guidance, such as NISTIR 8374 and SP 800-161 (see below for more on supply chain), into the Framework.

6. Use of non-NIST frameworks or approaches in conjunction with the NIST Cybersecurity Framework. Are there commonalities or conflicts between the NIST framework and other voluntary, consensus resources? Are there commonalities or conflicts between the NIST framework and cybersecurity-related mandates or resources from government agencies? Are there ways to improve alignment or integration of the NIST framework with other frameworks, such as international approaches like the ISO/IEC 27000-series, including ISO/IEC TS 27110?

We encourage NIST to continue to align with the ISO/IEC 27000 series, including by continuing to integrate ISO/IEC 27001 as an Informative Reference, and update ISO/IEC 27103 and ISO/IEC 27110 to be compatible with the Framework 2.0. Because those derivative approaches rest on a common security baseline of practices as well as a common taxonomy and lexicon,

organizations can build and maintain cyber risk management approaches that work across borders and industry verticals.[11] In addition, NIST could consider referencing industry standards from non-governmental standards development organizations, such as the Internet Engineering Task Force (IETF), Trusted Computing Group, and Global-Platform, especially in OLIR. Doing so would highlight commonalities or conflicts between NIST documents and widely used industry standards.

We also encourage NIST to partner with others across the U.S. government to ensure alignment in resources focused on critical infrastructure cybersecurity. For example, we recommend that NIST and CISA collaborate to leverage the Framework in developing the cross-sector baseline cybersecurity performance goals for securing control systems (developed in response to last year's National Security Memorandum of July 28). Doing so will promote the alignment of frameworks and security baselines for effective critical infrastructure protection, enabling greater consistency, clarity, and predictability, as well as focusing on and prioritizing organizations' cybersecurity assessment resources.

Furthermore, the alignment of best practice resources for critical infrastructure organizations helps foster consistency in best practice expectations and potential cybersecurity requirements, including those developed in the United States and internationally. Many U.S.-based critical infrastructure organizations are increasingly subject to cybersecurity regulation in the United States and globally. Fractured best practice resources (for which there is no explanation of how they are consistent, interoperable, and/or complementary) risk leading to operator confusion and fractured regulatory requirements, both in the U.S and globally. Each of the Common Baseline's performance goals and many of the objectives could be mapped to or aligned with the Framework v1.1 Core, including its Functions and Categories. For example, the Risk Management, Cybersecurity Governance, Architecture and Design, Configuration and Change Management, Physical Security, Data Protection and Access Control, Vulnerability Management, Personnel Training and Awareness, and Supply Chain Risk Management performance goals align with the Framework's Identify and Protect Functions; likewise, the Continuous Monitoring and Incident Response and Recovery performance goals align with the Framework's Detect, Respond, and Recover Functions.

In addition, we encourage efforts to define standardized relationships between domestic resources, including standards leveraged for security compliance programs. For example, last year, the North American Electric Reliability Corporation (NERC) released a mapping[12] between the Framework and NERC Critical Infrastructure Protection (CIP) Reliability Standards (NERC CIP). In addition to the mapping, NERC published a cybersecurity white paper explaining the benefits of this mapping, citing an International Energy Agency report[13] on cyber resilience in

[11] https://www.crx2.org/seamless-security-white-paper-press-release
[12] https://csrc.nist.gov/News/2021/updated-mapping-btwn-nist-csf-and-nerc-cip-stnds
[13] https://www.iea.org/reports/enhancing-cyber-resilience-in-electricity-systems

electricity systems that emphasizes the need to combine requirements-driven regulatory approaches with framework-based management strategies to ensure power grid cybersecurity.

Developing cross-sector Common Baseline performance goals that align with the Framework will further enable greater consistency, continuity, and predictability in the energy sector, in other sectors pursuing similar efforts, and in a cross-sector manner. Similar mappings or efforts to define standardized relationships with other security compliance programs would also raise awareness of successful uses of the Framework for such programs, a growing need in heavily regulated or soon-to-be regulated industries.

7. There are numerous examples of international adaptations of the Cybersecurity Framework by other countries. The continued use of international standards for cybersecurity, focusing on interoperability, security, usability, and resilience, can promote innovation and competitiveness while enabling organizations to integrate new technologies and services more efficiently and effectively. Given this importance, what steps should NIST consider to ensure any update increases international use of the Cybersecurity Framework?

Microsoft encourages NIST to continue to raise awareness of successful international adaptations of the Framework as well as aligned international standards and references, including ISO/IEC 27110 and ISO/IEC 27103. For example, Canada's Information Technology Security Guideline (ITSG)[14] is an excellent example of the Framework's flexibility to add unique controls while retaining the core scope. Another notable example is Infosec Registered Assessors Program (IRAP)[15] in Australia. Raising awareness of successful adaptations of the Framework may foster more robust community participation and crowdsource further international adoption. Further developing or promoting – or ensuring ongoing alignment of – international standards consistent with the Framework could also increase its global relevance and use.

[14] https://cyber.gc.ca/en/path-enterprise-security

[15] https://www.cyber.gov.au/acsc/view-all-content/programs/irap?msclkid=76192c41bef111ec85f79bf83b9fed1d

8. References should be considered for inclusion within NIST's Online Informative References Program. This program is an effort to define standardized relationships between NIST and industry resources and elements of documents, products, and services, and various NIST documents such as the NIST Cybersecurity Framework, NIST Privacy Framework, Security and Privacy Controls for Information Systems and Organizations (NIST Special Publication 800-53), NIST Secure Software Development Framework, and the NIST Internet of Things (IoT) Cybersecurity Capabilities Baseline.

Microsoft welcomes NIST's efforts to define standardized relationships between resources, including through the Framework's Informative References and OLIR. We are particularly supportive of efforts to reference international and industry standards, reference points, and best practices, helping to drive alignment across global cybersecurity risk management efforts. For example, including ISO/IEC 27001 in the Framework is especially valuable. In addition, we encourage efforts to define standardized relationships between domestic resources, including standards leveraged for security compliance programs. Going forward, we recommend that the Framework or OLIR as appropriate add or continue to support clarity regarding relationships with standards such as ISO/IEC 27103, ISO/IEC 29147, and ISO/IEC 30111 as well as standards developed by IETF, TCG, and Global-Platform.

In addition, alignment with Cybersecurity Maturity Model Certification (CMMC) and SP 800-171 Rev 2, Protecting Controlled Unclassified Information in Nonfederal Systems and Organizations, would significantly benefit US federal government contractors and help support approaches to security compliance grounded in cybersecurity risk management.

NIST describes the Framework as a living document that will continue to be updated and improved as the industry provides feedback on implementation. However, the Framework does not get updated when new Informative References are developed through the National Online Informative References (OLIR). Therefore, NIST should explore how the Framework community is updated when there are significant developments related to Informative References, even if Framework Core changes are not warranted. In addition, NIST should ensure that OLIR is referenced in Framework 2.0 as an additional resource for practitioners.

V. Cybersecurity Supply Chain Risk Management

Modern supply chains are complex, diverse, and constantly evolving, requiring technology- as well as people- and process-based supply chain risk management approaches. Modern systems combine software (including firmware), hardware, and services. Each comprises hundreds or thousands of individual components and supply chains in which producers and consumers have varying security postures. While increasing the baseline security of the whole supply chain is

ideal, we should also assume that this will take time and that there will be mismatches in suppliers' security postures and customers' security requirements. Misalignment of security requirements between consumer and supplier could occur because a consumer could have a different risk tolerance that does not match the supplier's product security specifications. Misalignment of consumer-supplier security requirements could be temporary, permanent, or systemic. Incomplete or inaccurate communication between consumer and supplier, changing environments, faults during implementation by the supplier, or usage by the consumer could all be causes of these misalignments.

To address cybersecurity supply chain risks, we must prioritize exchanging, correlating, and analyzing supply chain information. We also need to focus on optimizing for automatically detecting and responding to anomalies and support rapidly adapting to changing circumstances.

To address supply chain risks, the U.S. government is also evaluating availability and resiliency concerns. Microsoft has identified numerous challenges facing, for example, the semiconductor supply chain in its discussions with industry and government and in prior filings advancing the dialogue opened by the Administration with Executive Order 14017, America's Supply Chains.[16] For example, we submitted comments on November 8, 2021, in response to the Department of Commerce's Request for Public Comments on Risks in the Semiconductor Supply Chain, 86 FR 53031,[17] and in response to the Department of Energy's Notice of Request for Information on Energy Sector Supply Chain.[18] As noted in those comments, an array of obstacles, including long lead times, infrastructure constraints, and cost competitiveness, hinder the U.S. government's ability to address semiconductor supply chain challenges.

1. Integrate supply chain risk management into the Framework

Supply chain risk management is a cross-cutting issue that must be considered when addressing cybersecurity activities at their highest levels, i.e., Functions. Currently, the Supply Chain Risk Management (ID.SC) Category placed is located under the Identify Function, which the Framework describes as: Develop an organizational understanding to manage cybersecurity risk to systems, people, assets, data, and capabilities.

Microsoft recommends that this approach be revisited. Other Functions, such as Detect: Develop and implement appropriate activities to identify the occurrence of a cybersecurity event, should have associated cybersecurity supply chain risk management outcomes. Therefore, whether and how to include supply chain security should be considered across all five Functions of the Framework, not just the Identify Function. Doing so shouldn't mean that

[16] https://www.federalregister.gov/documents/2021/03/01/2021-04280/americas-supply-chains
[17] https://www.regulations.gov/comment/BIS-2021-0036-0091
[18] https://www.regulations.gov/comment/DOE-HQ-2021-0020-0088

supply chain risk management overwhelms the Framework; rather, it could result in a more cohesive and consistent approach throughout the Framework Core.

While Microsoft recognizes that how to effectively integrate supply chain security warrants further discussion among NIST multi-stakeholder community, below are some initial ideas for how existing supply chain risk management Subcategories could be better integrated across the Framework Functions and Categories. Consideration of additional Categories and/or Subcategories may also be warranted to increase alignment across NIST resources and U.S. cybersecurity policy developments, such as the SSDF and Executive Order 14028, as well as account for shifts in the ecosystem, including toward more organizations being both developers and consumers of software and other supply chain components and artifacts.

a) ID.SC-1: Cyber supply chain risk management processes are identified, established, assessed, managed, and agreed to by organizational stakeholders.

- Recommendation: Keep in Identify Function but move to the Governance Category

b) ID.SC-2: Suppliers and third-party partners of information systems, components, and services are identified, prioritized, and assessed using a cyber supply chain risk assessment process.

- Recommendation: Keep in Identify Function but move to the Asset Management Category.

c) ID.SC-3- Contracts with suppliers and third-party partners are used to implement appropriate measures designed to meet the objectives of an organization's cybersecurity programs and Cyber Supply Chain Risk Management Plan

- Recommendation: Keep in Identify Function but move to the Governance Category or Risk Management Strategy Category.

d) ID.SC-4: Suppliers and third-party partners are routinely assessed using audits, test results, or other forms of evaluations to confirm they are meeting their contractual obligations.

- Recommendation: Move to Detect Function's Monitoring Category.

e) ID.SC-5: Response and recovery planning and testing are conducted with suppliers and third-party providers.

- Recommendation: Move the response portion to the Respond Function and Response Planning subcategory and the recovery portion to the Recover Function and Recovery planning Category.

2. Automated and scalable attestation

As critical infrastructure and operational technology (OT) depend on more complex technology to meet modern needs, governments adopt commercial technology for sensitive use cases, and supply chains become more complex, we need to adopt new technologies to help secure the end-to-end supply chain at sufficient scale and speed. Some of these technologies are widely used in specific industries today (such as secure payments) but are applicable to securing general computing and protecting critical infrastructure.

The attestation of components and fully integrated systems are foundational to delivering trustworthy, resilient, and safe products/services to meet confidentiality, integrity, and availability requirements. Supply chains can be strengthened by using end-to-end attestation services to analyze systems from individual components (e.g., software, firmware, hardware) to complex assemblies in an automated and scalable fashion. To mitigate cybersecurity risks in systems, one must assure the authenticity of entities. Some approaches to authenticating entities are using evidence, policy, and artifacts to guarantee that an entity can be authorized, non-repudiable, immutable, and auditable.

Microsoft recommends that NIICS consider technologies such as remote attestation, hardware roots of trust, and trusted executed environments as critical to authenticating high-value assets, such as critical infrastructure, and their supply chains. We encourage NIST to facilitate multi-stakeholder engagements with standards groups working in this domain, such as IETF RATS[19] and Supply Chain Integrity, Transparency, and Trust (SCITT)[20], Trusted Computing Group (TCG), and the Confidential Computing Consortium (CCC), and develop guidance for applying these technologies to secure critical supply chains. NISTIR 8419 proposes a generalized blockchain for manufacturing supply chain traceability; however, for the cybersecurity supply chain use case, we recommend a Confidential Consortium Framework (CCF)[21]-based ledger using trusted execution environments (TEEs) to meet confidentiality, performance, transaction finality, and governance requirements.

3. Open source software security

It is critical for organizations to actively manage the security of their upstream suppliers. With commercial suppliers, this is often achieved through contractual agreements, third-party certifications, audits, or other assessment and monitoring processes. These processes require active involvement, and sometimes investment, from suppliers, which makes them ineffective or even impossible for open source dependencies.

Open source's unique model creates unique challenges for supply chain risk management. Open source is acquired at no cost and with a disclaimer of liability and warranty. Organizations

[19] https://datatracker.ietf.org/doc/charter-ietf-rats/
[20] https://datatracker.ietf.org/doc/draft-birkholz-scitt-architecture/
[21] https://www.microsoft.com/en-us/research/project/confidential-consortium-framework/

that have security requirements for open source projects need to convince the project to adopt those requirements or find ways to compensate for unmet requirements after consuming the open source software. Wide and deep dependency trees that can pull in hundreds of open source projects exacerbate this problem further.

Microsoft, along with a number of other companies, has partnered with the Open Source Software Foundation (OpenSSF) to identify, develop, and recommend approaches to securing open source software and their supply chains. We're proud to be one of the founders of the Alpha/Omega project at OpenSSF, which will work directly with maintainers of critical open source projects and identify automated security processes that can be applied broadly.

As an extension of investments in both the Framework and NIICS, we recommend that NIST considers the unique supply chain risk management challenges for organizations consuming (and producing) open source and provides guidance on how to tailor supply chain risk management processes to those scenarios. We recommend that NIST engage with open source communities, such as the OpenSSF, to develop and seek feedback on that guidance to ensure that it is feasible and reasonable.

Conclusion

Microsoft has been a committed partner throughout the Framework development process since it was initiated in 2013. We have collaborated extensively with domestic and international partners, including industry, NIST, and other government stakeholders. Our efforts have sought to ensure that the Framework approach incorporates insights gained through our experiences and partnerships with others and to promote awareness and implementation of the Framework. Microsoft is grateful for this opportunity to reiterate its commitment 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.

Respectfully submitted,

Patricia Ephraim Eke
Principal Security Strategist, Customer Security and Trust
Corporate, External & Legal Affairs
Microsoft Corporation