April 25, 2022

Katherine MacFarland
National Institute of Standards and Technology
100 Bureau Drive, Stop 2000
Gaithersburg, MD 20899

Re: Response to National Institute of Standards and Technology (NIST) Request for Information on Evaluating and Improving NIST Cybersecurity Resources: The Cybersecurity Framework and Cybersecurity Supply Chain Risk Management

Dear Ms. McFarland:

IBM appreciates the opportunity to respond to the National Institute of Standards and Technology Request for Information ("RFI") on *Evaluating and Improving NIST Cybersecurity Resources: The Cybersecurity Framework and Cybersecurity Supply Chain Risk Management*. IBM is a leading global enterprise technology and consulting company, serving clients in many industries, including financial services and other critical infrastructure sectors around the world. Cybersecurity is integral to IBM products and services. We provide clients with technology solutions, security consulting, threat intelligence and managed security services to address issues such as threat management, data security, identity and access, and fraud protection. We have demonstrated thought leadership on cybersecurity through publications, serving on advisory boards, and participating in workshops, panels and government and industry working groups, and recently launched the Center for Cybersecurity of Government to help government clients navigate the evolving cybersecurity threat landscape, leveraging IBM cybersecurity expertise and resources.

We applaud NIST's collaborative and open partnership with industry on cybersecurity. Since the Framework's inception, IBM has actively engaged with NIST to provide input on the development and evolution of the Framework. We also continue to participate in ongoing supply chain security initiatives, including NIST's initiative on software supply chain security pursuant to Executive Order 14028 on Improving the Nation's Cybersecurity (the "Executive Order on Cybersecurity"), and NIST's National Initiative for Improving Cybersecurity in Supply Chains ("NIICS.") We appreciate the complexity of these issues and encourage NIST to maintain the simplicity and flexibility of the Framework as NIST contemplates whether how to update the Framework to account for the evolving cybersecurity threat landscape. IBM offers the following response to NIST's request for comments, organized according to the themes laid out in NIST's RFI.

Usefulness of the NIST Cybersecurity Framework

The NIST Cybersecurity Framework provides organizations with a risk-based approach that is easy to implement. It provides a comprehensive methodology for organizations to ensure that basic foundational controls and processes are in place, monitored and continuously improved. The Framework's flexibility allows organizations of varying sizes and complexity to develop cybersecurity risk management programs that are appropriate to their respective levels of risk. At the same time, the Framework's Tiers and Profiles encourage organizations not only to assess their current cybersecurity posture, but also to identify aspirational outcomes. We strongly encourage NIST to maintain the simplicity and flexibility of the Framework so that it remains relevant and widely adopted around the world.

The Framework's five core functions provide a holistic approach to cybersecurity that all employees throughout an organization can understand. The interdependency of these five pillars and how they inform one another is key to the Framework's success and sustainability. Users of the Framework can measure their overall cybersecurity programs against these five functions to identify gaps, assess levels of risk, and determine where to allocate cybersecurity resources. Overall, the Framework provides a common structure and language for addressing cybersecurity risks within organizations, with customers, and throughout the supply chain.

IBM leverages the Framework in several ways. First, we use it to support our internal cybersecurity practices. For example, we base our own cybersecurity risk management program around the Framework and incorporate the Framework's five pillars into our internal cybersecurity policies and practices. Cybersecurity also is integral to the development of our products and services, and we leverage globally accepted frameworks, including NIST's Secure Software Development Framework ("SSDF") in our secure development process.

As a large enterprise security solution provider, we also leverage the Framework to support clients across multiple sectors to improve their own cybersecurity posture. Specifically, we help our clients use the five pillars of the Framework to identify gaps, develop long-lasting solutions to address those gaps, and institutionalize cybersecurity risk management throughout their organizations. The Framework's simple but comprehensive approach provides a flexible foundation that different organizations can utilize to improve their overall cybersecurity risk management.

Challenges of Using the Framework

Even though the Framework offers a simple and flexible approach to cybersecurity risk management, some organizations still may struggle with practical implementation. For example, smaller organizations may not have dedicated compliance teams or may have very small security teams. In addition, the Framework is exactly that, a framework, and less mature organizations may struggle with where to start, what to prioritize, and where to allocate limited funds. Simple user guides that provide practical implementation examples could be extremely useful to those organizations looking for more guidance on best practices. It also could be helpful to reiterate that the Framework is a risk

management tool, rather than a "check-the-box" compliance tool, and that organizations should continuously leverage the Framework to address evolving cyber threats. The Framework's outcomes-based approach also can serve as a model for updates to other Federal security approval processes that, in some cases, may become overly compliance-focused rather than aimed at addressing an organization's substantive security posture.

The overall structure and flexible approach of the Framework is key to its continued success, and we do not recommend fundamentally changing the Framework. We offer the following recommendations for NIST to consider in its efforts to update the Framework and improve cybersecurity in supply chains.

Recommendations:

Keep the Framework streamlined and flexible. The Framework is effective because it is simple and not overly prescriptive. It sets a strong foundation and gives organizations a flexible roadmap with essential signposts for managing cybersecurity risk. From the outset, the Framework was designed to be used by organizations of different sizes across multiple sectors and to accommodate changing technology and evolving cyber threats. While some organizations may benefit from implementation examples, we encourage NIST not to overcomplicate the Framework with more prescriptive requirements that will render the Framework more difficult to adopt and less relevant over time. To further support less mature or smaller organizations, NIST could consider developing implementation guidance, such as online workbooks, calculators, and risk assessment tools to help organizations with practical implementation. A particular focus on developing approachable and easily-digestible guides, such as NISTIRs, could help facilitate more widespread adoption of the framework throughout the digital ecosystem.

The Framework's five core pillars provide a comprehensive risk management approach that does not need to be expanded. Similarly, it is not necessary to introduce separate requirements for critical infrastructure. The Framework itself already contemplates the need to identify and manage differing levels of risk. Rather than complicating the Framework further with new requirements for critical infrastructure, it could be beneficial to specifically acknowledge the unique risks that critical infrastructure sectors may face and identify minimum standards for managing that risk.[1] Maintaining a flexible Framework that addresses a sliding scale of risk is key to its overall usability and widespread adoption.

Align the Framework to emerging trends, such as cloud. As the government (as recommended in the Executive Order on Cybersecurity), and many other critical sector entities accelerate their transition to cloud, it could be beneficial to review and update the Framework and associated NIST standards to address holistic risk management across all cloud environments, including hybrid and multi-cloud. As a leader in providing secure hybrid multi-cloud solutions, we encourage NIST to consider how the Framework could more specifically address the shared responsibility model, the cornerstone of cloud cybersecurity, to ensure that all participants in the cloud ecosystem adequately

[1] *See, e.g.* The White House, *National Security Memorandum on Improving Cybersecurity for Critical Infrastructure Control Systems* (July 28, 2021), https://www.whitehouse.gov/briefing-room/statements-releases/2021/07/28/national-security-memorandum-on-improving-cybersecurity-for-critical-infrastructure-control-systems/.

contemplate and clearly delineate respective roles and responsibilities for the various subcategories of the Framework. NIST also should consider updating its informative references, as appropriate, to include standards and best practices that are relevant to cloud environments, including AICPA SOC2 certification.

Align the Framework with other NIST risk management resources. We appreciate NIST's efforts align the Framework with NIST and other risk management resources. We encourage NIST to continue these alignment efforts, but caution against incorporating other risk management frameworks wholesale into the cybersecurity Framework. While it may seem ideal to have one comprehensive risk management framework that covers everything, the resulting framework would be unwieldly and difficult to implement, undermining the very goal of widespread adoption. What could be helpful is an extensive mapping exercise to identify linkages to and overlaps with other relevant NIST resources, such as NIST's SSDF, Privacy, and Artificial Intelligence Risk Management Frameworks. This could help implementing organizations identify a common subset of controls across the various frameworks that are relevant to them, while maintaining the value of separate frameworks that are focused on distinct risks.

Harmonize ongoing supply chain initiatives and incorporate supply chain risk management by reference. There are numerous ongoing initiatives to address cybersecurity risk in the supply chain, including NIST's work to update the SSDF, its recently launched National Initiative for Improving Cybersecurity in Supply Chains ("NIICS"), and the Department of Homeland Security's ICT Supply Chain Risk Management Task Force. It is not always clear whether and how these supply chain security initiatives relate to one another. We recommend that NIST consider and, where possible, harmonize the various government supply chain security initiatives through its NIICS efforts. Such alignment will help organizations adopt consistent supply chain cybersecurity principles within and across supply chains. We do not recommend incorporating these supply chain initiatives into the Framework itself. Rather the Framework should reference supply chain cybersecurity risk management as an essential component of the Framework and point to these evolving supply chain security resources and standards. NIST also could consider providing practical guidance on how organizations can allocate cybersecurity responsibility and accountability throughout the supply chain, including fostering industry consensus on supplier terms and responsibilities.

Consider providing additional clarity on Framework Tiers. We suggest that NIST consider providing additional clarity on the Framework's Tiers so that organizations have more objective criteria for assessing their current cybersecurity posture. This could be achieved, for example, through practical implementation guides on minimum criteria for each Tier. NIST also could consider mapping the Tiers to maturity levels. While we do not recommend that NIST establish maturity level requirements, mapping Tiers to maturity levels could be useful to those organizations that have determined their respective maturity levels and could help facilitate Tier assessment consistency across organizations.

Align the Framework with other globally accepted standards. There is a lot of overlap in security recommendations between the Framework and other global standards, such as the ISO 27000-series and others. In addition, the Framework itself is adopted by

organizations around the world. We encourage NIST to continue to engage in global outreach and align the Framework with other globally accepted standards. We note that adoption and use of Open Security Controls Assessment Language is one possible way to harmonize the mapping required between the Framework and other voluntary consensus-based resources.

Map the Framework to the Executive Order Cybersecurity. The Framework also can help government agencies by providing a common language that agencies can use to increase awareness of the importance of addressing the five pillars to enhance their overall cybersecurity posture. We encourage NIST to consider mapping the categories and subcategories of the Framework to the Executive Order on Cybersecurity. This could help demonstrate to government agencies how the Framework fits within the Executive Order on Cybersecurity and how it can help those agencies become more secure.

Ensure continuity and backward compatibility. Finally, NIST should take care not to impact the usability or backward compatibility of the Framework. Many organizations around the world already base their cybersecurity risk management programs on the Framework. We believe that NIST can improve the Framework (e.g. with enhanced mapping to other risk management resources, more specificity for the Tiers, and the publication of additional practical user guides) without creating compatibility issues for those organizations that already have adopted the Framework.

IBM appreciates NIST's continued engagement of industry and other relevant stakeholders as it considers updates to the Framework and improvements to cybersecurity in supply chains. We look forward to continuing to work with NIST on these important issues and welcome the opportunity to share our experience and expertise. The Framework sets a strong foundation for cybersecurity risk management that can be adopted by many organizations of different sizes and across different sectors. Maintaining the Framework's flexibility and simplicity is key to its continued relevance and widespread adoption.

Sincerely,

William Tworek
Vice President and Distinguished Engineer
Product Security
IBM Corporation
[redacted]