March 17, 2023

National Institute of Standards and Technology
100 Bureau Drive
Gaithersburg, MD 20878

VIA EMAIL: cyberframework@nist.gov

Re: IBM Response to National Institute of Standards and Technology (NIST) Cybersecurity Framework V2.0 Concept Paper: Potential Significant Updates to the Cybersecurity Framework

IBM appreciates the opportunity to respond to the National Institute of Standards and Technology Concept Paper resulting from last year's RFI responses to "Evaluating and Improving NIST Cybersecurity Resources: The Cybersecurity Framework and Cybersecurity Supply Chain Risk Management." We are grateful to NIST for continuing to be the model of public private partnership with continued collaboration going forward with review of concept papers and workshop discussions to help inform the next important version of the Cybersecurity Framework ("CSF") into V2.0.

IBM supports NIST's effort to update the CSF to better reflect the ever-evolving threat landscape and the emerging technologies and processes to defend and respond. The CSF was always meant to be a living document and V2.0 will be a huge proof point to adapt to current and future trends.

As we collectively continue this journey with the Cybersecurity Framework to further instantiate its critical importance to the U.S. and global cybersecurity ecosystem, IBM believes it is important to reinforce a few core tenants of the CSF as the process to update it moves along this year:

- Maintain simplicity and flexibility to account for the evolving cybersecurity threat landscape and for it to remain widely adopted globally. In other words, "don't break it" but continue to provide the considerations necessary for an organization to manage their cybersecurity risk and promote the online resources to help organizations with implementation.[1]

[1] *From IBM RFI submission April 2022: "The Framework's flexibility allows organizations of varying size and complexity to develop cybersecurity risk management programs that are appropriate to their business activities and 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."*

- Maintain its status as a "Framework" as it was purposely designed as such, 10 years ago, to inform organizations of the "what to do" not the "how to do it". Prescribing specific controls, actions, remediations, standards, etc. will quickly change the nature and intent of the CSF into a check the box compliance exercise[2]

As we mentioned in our RFI submission last year, IBM leverages the Framework both for our own cybersecurity risk management practices as well as to help clients improve their cybersecurity posture. CSF is not meant to be a standalone framework for industry to assess itself by and certify against, rather it is intended to be combined with other cybersecurity requirements for building comprehensive policies and processes. Consequently, IBM uses the CSF as a foundational framework for our policies and processes while also incorporating other NIST standards, regulatory requirements, and best practices. It is in the totality of these various requirements, which include MSAC, Internal Audit, ISO certifications, and third-party assessments, that we certify ourselves against. For these reasons, the CSF should remain broad framework and provide considerations for risk – not prescriptive measurements to comply.

IBM appreciates the importance of governance attributes as drafted in CSF 1.0 and understands the significance of including a new "govern" function. Nonetheless, while IBM supports NIST's efforts to highlight governance in V2.0, it is critical that any updates maintain CSF's original intent of broad applicability and non-prescriptive controls. Similarly, IBM supports NIST's inclusion of examples within V2.0 similar to how they are presented in SSDF, and further supports NIST's intent to ensure that examples be demonstrative and not prescriptive. IBM would encourage NIST to include language affirming the non-prescriptive nature of examples if they are included in V2.0.

While IBM supports a new "govern" function, we do not see a new "supply chain" function as an appropriate addition to the CSF. Overall, IBM encourages alignment or references to additional NIST resources within the CSF, specifically supply chain initiatives, and not full incorporation that could potentially devalue the "framework" attributes of the CSF. IBM believes that all the CSF functions can apply to an organization's supply chain, and as such, supply chain is a case of how and when to apply the various functions of the CSF based on the scope of the supplier, rather than supply chain being a new set of functions or practices.

As reflected in industry comments and in the concept paper, there are numerous ongoing initiatives to address cybersecurity risk in the supply chain. Industry clearly recognizes that cybersecurity is integral to the development of products and services as efforts like E.O 14028 is moving market forces demand for secure engineering/development as criteria for government purchase. As we conveyed in our RFI submission, "we do not recommend incorporating these supply chain initiatives wholesale 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." Bottomline, supply chain risk management should be considered throughout the Framework as an essential component (of the Framework) but not as a core function.

---

[2] *From IBM RFI submission April 2022: "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 purpose of the CSF is to guide an organization's cybersecurity preparedness while considering security risks associated with product development, rather than to stipulate how organizations must build secure products overall. If supply chain were categorized as a function, as discussed in the workshop, it would feel and appear as an outlier to the core five. Instead, NIST should consider the hybridized approach discussed during the February 22nd workshop, which would consist of incorporating C-SCRM requirements into the CSF by weaving various approaches, standards, frameworks, and so forth throughout the framework. This approach would allow the CSF to be considered as part of an organization's collective and comprehensive risk management program.

IBM appreciates NIST's continued engagement of industry and other relevant stakeholders as it considers updates to the Cybersecurity Framework. We look forward to reviewing the draft CSF V2.0 this summer and continuing to work with NIST on a final product for 2024.

Sincerely,

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