IBM®

November 6, 2023

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

SENT VIA: cyberframework@nist.gov
RE: IBM Response to Public Draft: The NIST Cybersecurity Framework 2.0

IBM appreciates the opportunity to respond to the public draft of the updated NIST Cybersecurity Framework (CSF V2.0) resulting from extensive stakeholder engagement since February 2022 to adequately and appropriately update the framework to reflect changes in technology and threat landscape. We applaud NIST's continued due diligence with industry through the RFI and extra opportunities to comment on discussion drafts and concept paper and NIST workshops to engage in dialogue. We congratulate NIST on producing a new draft that largely reflects industry commentary and perpetuating the model of effective public private partnership towards beneficial outcomes for both industry and government.

We reviewed CSF V2.0 draft with an eye on the areas IBM has commented on in previous iterations and are pleased with the changes reflected in the updated draft of CSF. However, there is still a core area of concern that we raised in our submission on the Concept Paper[1] that we must raise again to ensure that the CSF remains, as it always has been intended to be, simple and flexible to adapt to organizations risk posture. Our interpretation of CSF V2.0 seems to indicate that the CSF will be serving as an overarching framework for NIST cybersecurity guidance as it now incorporates many footnotes, NIST guidance docs and external references and point to "notional examples" some being very granular in nature.

This contradicts the intention of the CSF being simple, making it cumbersome and weighty and undermining the foundational purpose of the CSF to be a resource on "what to do" not "how to do it". Unlike the original CSF, this current iteration with numerous cross references to external materials, distracts from the framework itself and complicates the ability to interpret and understand the framework as a standalone document. While IBM previously suggested that there should be examples to illustrate various concepts, it is imperative that NIST do so in a demonstrative way to avoid creating a prescriptive model by which organizations will be evaluated against and/or drive regulators to interpret as compliance mechanism and eventually potential enforcement action. It is also worthwhile to mention that with the addition of the new Govern function, this slippery slope of interpretation as compliance check boxes could potentially open organizations to liability risk – an unintended consequence that would defy the spirit of the CSF entirely.

[1] 2023-03-17 IBM_508_redacted.pdf (nist.gov)

Therefore, we would like to reaffirm our request to NIST (as raised in past submissions and at 2 workshops) to decouple the CSF from the cross-references in order to maintain the high-level flexibility and adaptability of a single framework and preventing CSF V2.0 from being interpreted as an overarching framework with multiple frameworks, guidance, best practices, etc. included within. By linking these materials to CSF, for example, some of the NIST guidance documents (e.g., SSDF) will imply the entirety of those controls are part of the controls where referenced leading to confusion as to what an organization is being recommended to do.

We recommend that any external references be limited to the Implementation Examples Document to serve as the "how" for organizations to apply various aspects of CSF to their cybersecurity risk management programs. Moreover, the Implementation Examples Document should make clear that any examples provided are notional. We recommend that any use of "implementation examples" in the Implementation Examples Document refer instead to "notional examples" consistent with the CSF V2.0 Core Framework. Any cross-references currently incorporated within the CSF should be removed and reside exclusively within the Implementation Examples Document. Additionally, it would be helpful to include clarifying language around utility of profiles and guidance to reinforce that the CSF defines "what" needs to be done to reduce risk and therefore leaving the profiles, actions, and Implementation Examples Document as the "how". They may refer back to the CSF V2.0 themselves but the CSF should not point to the Implementation Examples, and contents thereof, specifically.

IBM thanks NIST for the open dialogue to contribute to this important effort and for taking our comments under consideration. We look forward to the final CSF V2.0 in 2024 and further partnering with NIST to propagate its use and international adoption. Please contact Katie Ignaszewski [redacted] with any questions or follow up.