

March 17, 2023

Via E-Mail: cyberframework@nist.gov

National Institute of Standards and Technology
Attn: Applied Cybersecurity Division, Information Technology Laboratory
100 Bureau Drive (Mail Stop 2000)
Gaithersburg, MD 20899-2000

RE: NIST Cybersecurity Framework 2.0 Concept Paper: Potential Significant Updates to the Cybersecurity Framework January 19, 2023 (the "Concept Paper")

Ladies and Gentlemen:

The Risk Management Association ("RMA") appreciates the opportunity to provide comments to the Concept Paper and welcomes the opportunity to convene members of its Operational Risk Council, Technology Risk Committee and other members to discuss the comments herein and other matters to assist in the development of the Concept Paper.

I. Background

RMA is a 501(c)(6) not-for-profit, member-driven professional association whose sole purpose is to advance the use of sound risk management principles in the financial services industry. RMA helps its members use sound risk management principles to improve institutional performance and financial stability, and enhance the risk competency of individuals through information, education, peer-sharing and networking. RMA has approximately 1,700 institutional members, which include banks of all sizes as well as non-bank financial institutions.

One of the most important components of RMA's mission is to provide independent analysis on matters pertaining to risk management and cyber regulation. In this regard, the comments contained herein are informed by subject matter experts from member institutions of RMA's Operational Risk Council and Technology Risk Management Committee.

General Observations

Governance

RMA supports NIST's initiative to enhance cybersecurity governance and notes that this initiative should provide institutions with sufficient clarity to enable the effective and efficient use of the framework. It is important to note that the framework should be implemented by institutions appropriately for their respective size, scale, complexity and breadth of operations. We would suggest that governance could be enhanced by providing guidance regarding cyber risk quantification, including the relationship to risk appetite. We also note that there appear to be conflicting directions between the NIST approach and other frameworks and methodologies.

Frameworks

RMA respectfully submits the current CSF 1.1 could be improved by providing guidance regarding when an institution should use a particular framework including the attributes of the competing frameworks that may be considered in making a determination. What are the risk-based attributes and sizing criteria to help organizations tailor CSF; what elements would smaller institutions scope out that would be in scope for larger institutions? RMA proposes that CSF 2.0 recommend institutional attributes when selecting a framework, such as the institution's size, maturity, complexity, and available expertise. RMA notes that smaller institutions may not have access to the resources or expertise to develop and/or implement a cyber risk management framework which can hinder the institution's effectiveness in managing cyber risk. Moreover, we recommend that the Standard would be improved by providing questions that institutions of varying size, scale or complexity should consider in tailoring the framework for their respective use.; this will help them to understand their relative maturity and resource constraints.

We note that there are several subcategories that can prove challenging to interpret due to potential overlap or the lack of specificity of implementation guidance, such as:

- ID.RA-1/DE.CM-8 – which cover the identification of vulnerabilities. Query how this should be interpreted by users. For example, under DE.CM8 scanning is one method of identification.
- PR.PT-7/PR.PT-8 – which each reference different kinds of integrity monitoring, but under the guidance speak to baseline processes which are not the same thing.
- ID.GV-4 – Governance processes are not defined by the framework. Is it meant to be overarching program governance, or each sub program (IAM, EA, SDLC, Vuln Management, etc.)?
- Across the DE/RS/RC sections, the actions taken to respond to an incident on an end-to-end basis are blurred and unnaturally bifurcated across these subcategories, most notably items related to communications, which makes for challenging mapping to processes, controls, and conducting meaningful benchmarking activities.

Accordingly, we respectfully recommend re-evaluating the group and bifurcation of the subcategories to ensure better alignment to end-to-end processes (and how they would actually play out within an enterprise). We also recommend ensuring that the referenced guidance adequately supports the intention behind the subcategory statements.

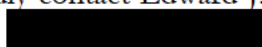
Vendor or Third Party Risks

Institutions will naturally use vendors or other third parties in managing cyber risk, as well as providing other services. The Standard would be improved by highlighting the interplay among cyber risk, third party risk and operational resiliency and by highlighting the very real possibility of concentration risk among critical vendors such as cloud providers where there is very little in the way of alternative vendors which impacts not just industry participants but institutions in wholly unrelated industries many of whom could be characterized as participants in private critical activities such as finance,

energy, transportation, food, drug and the like. We note that it is exceedingly difficult for institutions to migrate from vendor to vendor with significant effort, cost and other challenges.

Conclusion

RMA appreciates the opportunity to provide these comments and thanks NIST for its continued engagement with RMA's membership in studying cybersecurity. RMA looks forward to continuing its engagement with the NIST on these issues and would be pleased to facilitate a meeting between NIST and members of RMA's Operational Risk Council and Technology Committee.

Should there be any questions concerning the comments reflected above, kindly contact Edward J. DeMarco, Jr., Chief Administrative Officer and General Counsel at 

Sincerely,



Edward J. DeMarco, Jr.
Chief Administrative Officer & General Counsel