Risk Management Association

Advance Your World.

March 10, 2022

Via E-Mail nistir8286@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: Draft NISTIR 8286C, Staging Cybersecurity Risks for Enterprise Risk Management and Governance Oversight

Ladies and Gentlemen:

The Risk Management Association ("RMA") appreciates this opportunity to respond to and inform the Draft NISTIR 8286C, Staging Cybersecurity Risks for Enterprise Risk Management and Governance Oversight ("8286C" or the "Standard").

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 and capital 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.

RMA's comments are divided into two separate sections: Section II provides general observations and commentary about the Standard, while Section III provides RMA's responses to the discrete questions posed in the Standard.

II. General Observations

RMA supports NIST's initiative to ensure the incorporation of cyber risk into enterprise risk management and governance oversight to enable a deeper understanding of cyber risk as it pertains to its threats, impacts and the necessity for investment. As a threshold issue, RMA believes that the management of cyber risk should not be static and backward-looking; i.e., documenting and reporting what happened. Rather, it should be forward-looking and allow for those working directly within the cyber security world, senior management, and boards of directors to understand the threat vectors; the nature of threats; and the impact on the business in terms of risk, investment, and impact so that organizations can manage the financial impacts of cyber risk.

RMA believes that the Standard could be improved by addressing key risk management principles and providing a common risk taxonomy. In addition, it should incorporate industry-developed frameworks and white papers as appropriate to assist organizations in operationalizing the Standard. RMA believes that the readability and comprehension of the Standard would be improved by the addition of a "definitions" section at the beginning of the Standard, which could be placed after the Summary or to refer back to the definitions in NISTIR 8286 if all terms are defined in this earlier Standard. Furthermore, RMA also notes that Appendix A to NISTIR 8286C contains a list of approximately 30 acronyms and abbreviations and recommends referencing to NISTIR 8286 for the glossary.

RMA believes that the Standard could be improved by incorporating the concept of risk appetite and risk tolerance as defined within NISTIR 8286. In order to effectively manage cyber risk on an enterprise-wide basis, organizations should consider their appetite for cyber risk[1]. An organization should develop its annual operating plan and budget within the constraints of the appetite and tolerance for risk. This ensures that the organization does not exceed its stated bounds or limits for risk, as illustrated on Exhibit A. This treatment is consistent with the approach taken by COSO[2], which defines the terms "risk appetite" and "risk tolerance" as follows:

- Risk Appetite is "the amount of risk, on a broad level, that an organization is willing to accept in pursuit of stakeholder value."

[1] RMA has defined the term "risk appetite"[1] as the amount of risk (volatility of expected results) an organization is willing to accept in pursuit of a desired financial performance (return). RMA notes that the concepts of risk appetite and risk tolerance are often used interchangeably but have distinct differences in meaning. "Risk tolerance" encompasses the broadest expression of risk an organization is willing to assume in executing its strategy. Risk appetite offers a pragmatic view of risk tolerance.

[2] COSO – The Committee of Sponsoring Organizations, whose mission is to provide thought leadership through the development of frameworks and guidance on enterprise risk management, internal controls, and fraud deterrence.

- Risk Tolerance "reflects the acceptable variation in outcomes related to specific performance measures linked to objectives the entity seeks to achieve."

Risk appetite serves as the basis for an organization's risk governance framework, containing qualitative components that define a safe and sound risk culture and how the organization will assess and accept risks and quantitative limits that include sound stress testing processes and address earnings, capital, and liquidity.

RMA notes that the Standard appears to use the terms "technology risk" and "cyber risk" interchangeably. RMA respectfully suggests that the Standard could be enhanced by clearly differentiating the definitions between technology risk and cyber risk by including a definition of technology risk.

III. Responses to Questions Presented

1. **Is the use of risk criteria for risk reporting, escalation and elevation, and the normalization of cybersecurity risks at the organizational and enterprise level effectively discussed?**

   Generally, the use of risk criteria for risk reporting, escalation and elevation, and the normalization of cybersecurity risks at the organizational and enterprise level is effectively discussed. However, as stated in Part II of this response the Standard would be enhanced by effective cross-reference to 8286A and 8296B, as well as clear definitions of and distinction between the terms "cyber risk" and "technology risk," which appear to be conflated in the Standard. It is important to tailor the definitions of the two terms because an organization cannot effectively manage and report on a risk absent a common and well-defined taxonomy.

   In addition, the Standard could be enhanced by more clearly articulating the normalization concept discussed in 8286A because the of the importance of risk appetite and risk tolerance in relation to the concept of normalization. RMA notes that each scenario represents a specific loss event that should be evaluated in terms of an organization's risk appetite and risk tolerance.

   Moreover, the Standard supports a bottoms-up, decentralized approach to risk articulation, in lieu of a top-down approach. RMA respectfully submits that a de-centralized, bottoms-up approach to risk articulation will result in designation of similar risks with different taxonomies making it difficult to aggregate "cyber risks" across the breadth of the enterprise, with the result that a clear holistic view at the top of the house will be difficult, if not impossible. RMA recommends that the development of the risk framework come from the top down, but the identification and day-to-day management arise from the bottom up as the Standard currently is written. It is with the dual approach that risk can be most effectively managed.

2. **Have the differences and distinctions between risk aggregation, deduplication, normalization, optimization, and prioritization been made clear?**

   While the differences have generally been made clear, further guidance or clarity regarding the concept of deduplication is warranted. It is unclear whether the concept of deduplication is intended to rationalize, harmonize or eliminate the same risk scenario intended to be utilized by two different business units. For example, in the case of ransomware, the organization may likely have multiple scenarios impacting different systems and may want to aggregate the impact of all those scenarios by combining each into one common scenario.

   RMA respectfully suggests that the Standard could be improved by including additional context to the aggregation of risk response column approach outlined on page 14 (lines 486-489). Each of these costs at a "system level" should be considered in light of what the risk response is (e.g., whitelisting external internet addresses or software) and what the response is for (e.g., ransomware). If there are multiple ransomware scenarios in the risk register, and multiple "whitelisting" responses to address each risk scenario, each of the "whitelisting" costs needs to be considered, validated, and not double counted since implementing whitelisting would impact the entire enterprise. In this case, lines 486-489 suggesting using a "statistically weighted average of the risk response costs" (e.g., implementing whitelisting for each scenario) may be appropriate. RMA again emphasizes that organizations need to have a clear, well-articulated risk taxonomy and normalized data across all of the risk stripes to ensure a holistic enterprise-wide view of the risks.

3. **Is there existing industry guidance that would inform the format and content of Enterprise CSRR and the Enterprise Risk Profile?**

   A threat could be manifested across various risk types such as a technology risk, information security risk, fraud risk, or reputational risk. Accordingly, RMA suggests that the Standard would be significantly enhanced for financial institutions or other similarly regulated institutions and for third parties that engage with the regulated sectors by referencing the following frameworks and white papers developed by RMA through its Operational Risk Council, Enterprise Risk Management Council and Technology Risk Committee:

   - ERM Framework
   - Risk Appetite Workbook
   - Operational Risk Management Framework
   - Technology Risk Framework
   - Strategic Risk Framework
   - Reputation Risk Framework

   RMA has considered the risk environment in which organizations operate not just the control environment. RMA respectfully suggests that the Standard could be enhanced by including express reference to other industry guidance such as the RMA frameworks and

white papers noted above (accessible to RMA members) to assist end users implement the general principles articulated by the Standard.

4. **Are organizational responsibilities for the conveyance of cybersecurity risk information to the enterprise level effectively and clearly described?**

   RMA suggests that the Standard could be improved by highlighting the core responsibilities of senior management, the management of business lines, and independent risk management on their respective core responsibilities with respect to cyber risk. A core principle of effective senior management requires that clear responsibilities and accountability be established for the identification, measurement, management, and control of risk. We also note that senior management is responsible for providing timely, ***useful*** (emphasis added), and accurate information to the Board and leadership.

   In discharging their risk oversight function, boards should monitor the entity's performance against risk appetite and other metrics established pursuant to key policies approved by the board or its committees. Boards and leadership should be receiving high level information and key risks of concern in the context of informative and actionable reports from management. However, it is management, which is responsible for managing risk, not the board which is charged with risk oversight and business line management should execute business line activities consistent with the organization's strategy and "risk appetite."

5. **Does the reputation risk analysis help you see and perhaps respond to different stakeholders' impacts on valuation, volatility, and other enterprise issues?**

   The Standard conflates the concepts of risks and impacts of risks that materialize, which result in reputational risk. The Standard could be enhanced by clearly articulating the difference between risks and impacts. For example, the unauthorized access to information (a "risk") could result in class action litigation (legal risk within a defined risk taxonomy) and an unfavorable result could then lead to increased regulatory scrutiny, higher cost of capital, decreased consumer sentiment (all impacts).

6. **Does NISTIR 8286C provide sufficient information to inform different stakeholder groups' sentiment analysis and reputation consequences?**

   RMA does not believe that the Standard provides sufficient detail or information to provide clear and meaningful guidance to end users. Despite the importance of an organization's reputation, there are few tools for managing the risk to it. Moreover, risk managers take divergent views on managing reputation risk, with one camp classifying reputation risk as a stand-alone risk while others seeing it as a consequence or byproduct of the manifestation of other risks. Regardless of its taxonomy, reputation risk is dynamic—not static—and risk managers must play a role in maintaining, protecting, and, if necessary, repairing a firm's reputation with its stakeholders. RMA respectfully suggests that the Standard could be greatly enhanced by expressly referencing RMA's Reputational Risk Framework and associated white paper.

7. **Are common challenges in the translation of cybersecurity risks to enterprise level impacts adequately addressed (e.g., via the CSF mapping)?**

   The Standard could be improved by noting that the distinction and relationship between technology risk, cyber risk and third-party risk. Because the Standard uses the terms technology risk and cyber risk interchangeably, precise definitions are needed (See Comments in Part II above). In addition, because cyber risk can emanate from an organization's third parties and their subcontractors, the Standard could be improved by clarifying factors if a breach should be attributed to a third party is a "cyber" risk or a "third party" risk for purposes of risk identification, aggregation, management and reporting.

   In addition, the risk "impact" factors on page 18 (Figure 4) should be clearly delineated as primary or secondary impacts, and the alignment of cybersecurity risks to enterprise impacts should be made clear. To some extent, CSF steps are helpful in providing an overview of the cybersecurity improvement process, but greater alignment with to confidentiality, integrity, and availability loss risks at an enterprise taxonomy level would be helpful and would align the Standard with NIST 800-53.

8. **As NISTIR 8286C completes the description of the CSRM/ERM integration life cycle, what additional related topics would be helpful to readers?**

   The Standard would be improved by clarifying that risks should be well understood (for example though the risk and control assessment process or the use of scenarios) and documented prior to a line of business taking action that would expose an organization to such risks when every possible. Moreover, it should be well understood, documented and timely reported to senior management when risks will or may exceed the organization's risk appetite and approach its risk tolerance.

9. **Does the draft sufficiently help an entity consider the various roles and responsibilities for integrating CSRM and ERM?**

   Subject to the comments above and hereinafter, RMA supports the Standard and believes that it offers sufficient information, for an organization to consider the various roles and responsibilities for integrating CSRM and ERM, particularly when read in conjunction with other industry-specific resources such as the RMA Frameworks noted above.

10. **Are the key elements of cybersecurity risk evaluation, monitoring, and adjustment represented?**

    Subject to the comments provided throughout this response, RMA recommends that the standard be enhanced to provide insight into the role of risk identification prior to evaluation, monitoring and determining what, if any, adjustments are warranted.

11. **Does the publication effectively relate to both private and public sector enterprises in its structure, terminologies, and examples?**

Subject to the comments above and hereinafter, RMA supports the Standard and believes that it effectively relates to both private and public sector enterprises in its structure and terminology. RMA suggests that the Standard would be enhanced further by expressly referencing available industry resources such as the RMA Frameworks and white papers. RMA notes that here are many existing industry practices in place across public and private sectors and referencing to these practices, may make the NIST document more useful to users.

12. Throughout the NISTIR 8286 series, has a clear definition and understanding of "positive risk" been presented along with clear and helpful examples?

The concept of positive risk is counterintuitive and seems to imply an unexpected or unintended consequence of a risk that does not nor could not lead to a loss. The Standard would provide greater clarity to the reader to speak in terms of risk mitigants and the impacts, consequences, or results of a risk to which a mitigation strategy has been applied.

13. Does the NISTIR 8286 series provide sufficient information to generate a form that would enable effective comparisons between cyber risk and other non-cyber risk consequences and concomitant resource allocations?

RMA respectfully submits that the Standard falls short in providing sufficient information to generate a form that would enable effective comparisons between cyber risk and other non-cyber risk consequences and concomitant resource allocations. Such a form would need to enable non-cyber experts to make an informed decision across risk stripes. The Standard would be significantly enhanced by the creation of a template/sample form to aid understanding of the concept and how its use aids implementation of the Standard's concepts.

14. Does the information outlined in the NISTIR 8286 series provide sufficient information to inform SEC/IRS disclosures regarding financial statements and MDA narratives?

RMA respectfully submits that the Standard falls short in clarity and in providing sufficient information to inform SEC/IRS disclosures regarding financial statements and MDA narratives.

15. Do you think the NISTIR 8286 series provides sufficient information to enable the allocation trade-offs of an organization's operating expenses (OpEx) and capital expenditures (CapEx) for cyber issues and among non-cyber risk issues?

The NISTIR 8286 series does not appear to provide sufficient information to enable the allocation trade-offs of an organization's operating expenses for cyber issues and among non-cyber issues. While this is ultimately a determination made by an organization's finance unit, broadly speaking the conflation of the terms technology risk and cyber risk as described above make this allocation more difficult. Investments in what may be deemed

"technology" would likely be capitalized while expenses associated with addressing "cyber risk" such as the purchase of cyber insurance or the payment of ransomware would be expensed in the period in which incurred. RMA recommends that the Standard not provide finance related guidance and remain focused on ensuring cyber risk is well integrated into the broader risk framework.

* * * * *

In conclusion, RMA supports NIST's goal of harmonizing the cyber risk and enterprise risk management and governance believes that the final published Standard would be greatly enhanced by addressing key risk management principles and providing a common taxonomy and should incorporate industry-developed frameworks and white papers as appropriate to assist organizations in operationalizing the Standard. Should there be any questions concerning the comments reflected above, kindly contact Edward J. DeMarco, Jr., Chief Administrative Officer and General Counsel at (215) 446-4052 or edemarco@rmahq.org.

Once again, access to the RMA frameworks referenced in this document is available to RMA members. Should you encounter any difficulties with reviewing these documents, please contact the undersigned.

Very truly yours,

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

EXHIBIT A