From: Craig, Whitney <wcraig@rims.org>
Sent: Wednesday, October 23, 2019 1:24 PM
To: privacyframework <privacyframework@nist.gov>
Cc: Fox, Carol <cfox@rims.org>; Cain, Julie <jacain@ets.org>; Mandel, Chris <chris.mandel@sedgwickinstitute.com>
Subject: NIST Privacy Framework: Preliminary Draft Comments

Dear all,

RIMS appreciates the opportunity to offer comments on the NIST Privacy Framework preliminary draft. Our comment letter is attached.

Regards,

Whitney Craig

Whitney B. Craig

Director, Government Relations

RIMS | the Risk Management Society

October 23, 2019

Via privacyframework@nist.gov

Re: **NIST Privacy Framework: Preliminary Draft Comments**

Comments of the Risk Insurance Management Society

The Risk Insurance Management Society ("RIMS") appreciates the opportunity to comment on the "NIST Privacy Framework: A Tool for Improving Privacy Through Enterprise Risk Management (ERM)". As the preeminent organization dedicated to promoting the profession of risk management, RIMS, the risk management society®, is a global not-for-profit organization representing more than 3,500 industrial, service, nonprofit, charitable and government entities throughout the world – all of which are purchasers of commercial insurance. As such, RIMS' members are concerned deeply about improving privacy though ERM.

The NIST Privacy Framework draft reflects an encouraging development especially in alignment with NIST CSF, evidence that COSO ERM 2017 was considered and importantly, explicit recognition of and clear desire to reinforce an enterprise risk management (ERM) approach to privacy risk and its implications for organizations and individuals. This broader construct is an encouragement to the professional risk manager, a key organizational leader who are our primary constituents.

Governance and Risk Management:

Risk professionals would find even more encouragement in this framework if it clearly recognized the importance of leading with governance consistent with other risk related framework and standards such as COSO ERM 2017, ISO 31000, among others that are already in place and often mandated in mature organizations. Boards are looking for consistency and assurance. Explicitly aligning to these standards and acknowledging their foundational importance in support of effective governance will go a long way in easing broad adoption of this privacy framework inclusive of government as well as public and private industries.

Specifically, the five functions outlined in section 1.1 begin with identification followed immediately by governance. This order supports a more bottom up, technical analysis versus a top down, leadership view that would emanate from a properly designed and functioning risk culture orientation. RIMS proposes that these functions begin with governance to support the organizational context and standards-aligned guidance necessary to execute the framework well. Governance would then be immediately followed by identification.

1407 Broadway, 29th Floor, New York, NY 10018
t 212.286.9292 ■ f 212.655.5931 ■ www.RIMS.org

Issues that RIMS suggest you consider in support of this alternate approach include the following:

- Governance for privacy includes developing a strategy to integrate with the organization's overall standards-aligned governance and risk management structure
- Privacy risk tolerance should be one of the first things established in order to understand and put in context the organization's privacy exposure
- In establishing privacy risk tolerance, it should be aligned with the appetite for privacy risk which fits each organization, and which then makes clear the desired state for privacy risk acceptance
- Mechanisms for determining organizational privacy risk appetite and tolerance should be aligned to the organization's overall governance and risk management approach
- This approach supports a more horizontal versus vertical design
- This order of execution would better reinforce the role of the risk leader in the organization and their role in ensuring the effective management of privacy risk
- The existing order with "identify" first is inconsistent with COSO ERM 2017 and other risk standards and frameworks which typically lead with governance and follow with strategy
- The proposed approach will be particularly useful for financial institutions most of whom are committed to COSO for their approach to ERM
- This approach will also reinforce the board's risk oversight requirement including clarifying:
    - Where in the organization, privacy exposure exists
    - How and where cross functional collaboration should occur among and between a Privacy Office, the Chief Risk Office and the operational risk leader
- This approach would reinforce the gold standard of "privacy by design" not default
- This approach will drive a more direct connection to the broader risk strategy and framework
- This approach will improve the privacy risk attitude or posture for other than fear driven motivations
- This approach will strengthen the second line of defense/accountability

Finally, we believe that this modest adjustment to your draft framework will reduce market/user confusion over priorities in risk management process execution.

RIMS appreciates the opportunity to comment on the Framework. If you have any further questions, please feel free to contact Carol Fox, RIMS Vice President of Strategic Initiatives at cfox@rims.org.

Sincerely,

Gloria Brosius, RIMS-CRMP
President, RIMS Board of Directors