From: Margaret Murphy <mamurphy@utica.edu>
Sent: Thursday, October 24, 2019 4:12 PM
To: privacyframework <privacyframework@nist.gov>
Subject: NIST Privacy Framework: Preliminary Draft Comments

National Institute of Standards and Technology
100 Bureau Drive, Stop 2000
Gaithersburg, MD 20899

National Institute of Standards and Technology,

This letter is in regard to providing preliminary draft comments, for the NIST Privacy Framework: A Tool for Improving Privacy 87 through Enterprise Risk Management.

The principles within the draft that are focused on addressing diverse privacy needs are excellent, and show a strong foundation through the incorporation of (1) the design and deployment of systems, products and services, (2) the integration of privacy practices within business practices, and (3) the effective communication about these practices.

The NIST Privacy Framework also shows a strength by incorporating cross-organization collaboration and adaptability within each organization. The primary components of the NIST Privacy Framework: (1) Core, (2) Profiles and (3) Implementation Tiers; reinforce risk management within the scientific industry as well as the government. The Implementation Tier is an important component within each industry's review process, and could become a measurement for industry specific risk informed responses.

The NIST Privacy Framework also includes important components that define privacy in terms of (1) Cybersecurity Risks and (2) Privacy Risks. Cybersecurity Risks are defined as risks that are associated with a loss of confidentiality, integrity or availability. Privacy Risks are defined as risks that are associated with unintended consequences of data processing. This seems to be an important differentiation, because of the current debates in the field that are based on the extent of privacy that should be accorded to each individual. Through an updated definition of privacy, the dedication to develop secure technology can continue, without being stopped by debates in the field.

The inclusion of the Privacy Risk Assessment is also an excellent method to address security risks. The focus on identifying, evaluating, prioritizing and responding to specific privacy risks will help organizations to determine appropriate responses, which can reduce response time. By reducing response time, organizations can leverage their response procedures with remediation procedures, and make the attack surface less penetrable.

Privacy Risk Assessments are also a valuable consideration because they can help an organization to understand the values to protect, the methods to employ, and the way to balance the implementation of different types of measures.

As an early career researcher, in the process of applying to my PhD, I appreciate the importance of protecting sensitive information and scientific research; and how sometimes the two are part of the same organization. Thank you for publishing the NIST Privacy Framework, so that scientists can also review the NIST structure and incorporate these components within their work.

Best Regards,
Margaret Murphy