Katie MacFarland
Re: RFI concerning "Developing a Privacy Framework"
January 10, 2019

Karen Greenhalgh, HCISPP
Managing Principal
Cyber Tygr

Healthcare and Public Health, designated as a national critical infrastructure sector[1], has embraced the voluntary NIST Cybersecurity Framework to augment HIPAA compliance. Cyber Tygr, dedicated to helping healthcare providers create a culture of security and improve HIPAA compliance for privacy and security, anticipates this Privacy Framework will have an equally significant impact.

The recent revision of NIST SP 800-37, Risk Management Framework for Information Systems and Organizations - A System Life Cycle Approach for Security and Privacy [2](NIST-RMF) addresses the need to coordinate information security and privacy. Also, NIST-RMF states "…the NIST Cybersecurity Framework (NIST-CSF) can be aligned with the NIST-RMF and implemented using NIST risk management processes." Therefore, I offer two suggestions concerning the Structuring of the Privacy Framework:

- Just as the NIST-CSF and NIST-RMF can be aligned, so should the NIST Privacy Framework. Ideally, the Privacy Framework development will parallel the Cybersecurity Framework structure of functions, categories, and subcategories, allowing detail with clarity. Following the familiar format of the Cybersecurity Framework will leverage an organization's existing investment in the Cybersecurity Framework, particularly those in the healthcare industry.
- To assist the coordination of the Cybersecurity Framework with HIPAA, HHS worked with NIST to create the HIPAA Security Rule Crosswalk to the NIST-CSF[3].The Cybersecurity Framework is in accord with the HIPAA Security Rule; the Privacy Framework should be in accord with HIPAA's Privacy Rule. Developing a HIPAA Privacy Rule Crosswalk to NIST Privacy Framework along with, or soon after, publication of the Privacy Framework will assist incorporation of the Privacy Framework into existing cybersecurity programs.

[1] Presidential Policy Directive 21 (PPD-21): Critical Infrastructure Security and Resilience
[2] https://csrc.nist.gov/publications/detail/sp/800-37/rev-2/final
[3] https://www.hhs.gov/sites/default/files/nist-csf-to-hipaa-security-rule-crosswalk-02-22-2016-final.pdf