From: Matthew Bernstein <matthew@bernsteindata.com>
Sent: Thursday, October 24, 2019 4:37 PM
To: privacyframework <privacyframework@nist.gov>
Subject: Comments on the Preliminary Draft of the NIST Privacy Framework

MC Bernstein Data helps companies meet and maintain their information governance risk and business objectives. Privacy is our clients' primary concern at this time. The NIST Framework is an important milestone in enabling that dialogue. Thank you for the opportunity to comment. Our comments are attached.

Matthew Bernstein

matthew@BernsteinData.com

Phone: +1-646-893-1663

MCBERNSTEIN DATA_Horiz_web

BernsteinData.com

October 24, 2019

National Institute of Standards and Technology (NIST)
Attention: Katie MacFarland 100 Bureau Drive, Stop 2000
Gaithersburg, MD 20899

Submitted electronically to: privacyframework@nist.gov

RE: Request for Comments on the Preliminary Draft of the NIST Privacy Framework

Dear Ms. MacFarland:

MC Bernstein Data commends the efforts of NIST to-date in developing this Framework. We attended the Workshop in Atlanta this spring and we look forward to contributing to the development of the Framework in future.

We believe the importance of this work is most critical in addressing a gap that is identified in the Executive Summary, as part of setting out what the "Core" of the Framework enables, but which has much broader benefits. At the center of a necessary business and regulatory consensus on what "data privacy" means is: "a dialogue—from the executive level to the implementation/operations level—about important privacy protection activities and desired outcomes."

MC Bernstein Data helps companies meet and maintain their information governance risk and business objectives. Privacy is our clients' primary concern at this time. The NIST Framework is a milestone in enabling that dialogue. Thank you for the opportunity to comment.

General Comments

The Executive Summary to the Framework document states that (emphasis added):

> "The Privacy Framework—through a risk- and *outcome-based approach*—is flexible enough to address diverse privacy needs, enable more innovative and effective solutions that can lead to better outcomes for individuals and enterprises, and stay current with technology trends..."

Our specific comments below are all addressed to this point: we believe the Framework document should have fewer suggested management processes and programs, and add value to organizations' management of data privacy by providing valuable guidance on "What" they should consider doing, rather than "How" they should do it; the "outcome-based approach" advocated by NIST itself.

Specific Sections

A. Section 2.1 Core and Appendix A Subcategories GV.MT-P7 and CT.PO-P3

Section 2.1 defines five Functions. The definitions describe the critical activities in each Function for enterprise management of Privacy risk. None of the definitions (in this important introduction to the what the Framework supports) mentions responding to individuals' requests regarding their data, such as preferences or access. The obligations of organizations ***to*** individuals is a central development and tenet of current and evolving privacy laws, regulations, and policies. This critical responsibility should be elevated in overall prominence and, at the very least, cited in this defining section.

While processes related to these obligations are touched upon in Subcategories GV.MT-P7 and CT.PO-P3, more detail should be given to the typical and particular obligations, such as the individual's rights regarding data portability, data access, third-party transfer, and data erasure; other Framework Subcategories provide guidance for smaller issues at a much more granular level.

B. Section 2.3 Implementation Tiers and Appendix E: Implementation Tiers Definitions

The Tiers as developed describe qualitative "states" of an organization, rather than the presence/lack of the governance, processes, people, and technology capabilities (the standard components of a Target Operating Model) necessary to manage privacy risk. The Tier levels are both too subjective and do not describe the organization's Current or Target Risk Management posture.

At the very least, the definitions in Appendix E should be based on the adequacy of the user organization's Framework Functions Categories/Subcategories. E.g., "Repeatable" might mean all relevant Subcategories have been evaluated and found to be incorporated into "Business as Usual" functions of the organization.

C. Section 3.3 Establishing or Improving a Privacy Program

Similar to the comment regarding the risk assessment (see E, below), this guidance may be useful if the organization does not have Program or Change Management frameworks and approaches, but it is not a standard change management rubric, may be for organizations to adopt, and is a domain for which many other frameworks are already in use.

D. Section 3.5 Using within the Data Processing Ecosystem

The entities shown should be both more generic and take into account that the "ecosystem" in almost every organization is not entirely internal. We suggest eliminating "Manufacturer" and "Commercial Product/Services", and adding "Lines of Business", "Internal Data Stores/Processes", and "External Data Stores/Processes" (e.g. 'cloud' providers).

E. Appendix D – Conducting Privacy Risk Assessments

Consideration should be given to eliminating this section. While it is helpful "[i]f an organization is not using a pre-defined risk model", this is one of the areas of the Framework document that has the potential not to resemble organizations' existing (and adequate) overarching risk management operating models and thus unintentionally create a "gap" where none really exists. Again, we believe this "How" is not necessary.

The "Risk Model" guidelines of this section (pg. 36) do not present a clear and standard (risk management) relationship among the three NIST Privacy Risk Factors and the graphic is not helpful (Problematic Data Action | Likelihood | Impact). A standard view of enterprise risk would equate them as follows: Likelihood X Impact = Problematic/Non-problematic Data Action. The results of such a calculation (which could be linear, not binary) would allow risk management decisions to be taken and resources appropriately allocated.