October 24, 2019

Via Electronic Mail

The Honorable Walter G. Copan
Under Secretary of Commerce for Standards and Technology and NIST Director
U.S. Department of Commerce
Washington D.C. 20230

Re: *NIST Privacy Framework: Preliminary Draft Comments* (84 FR 47255)

Dear Dr. Copan:

The Bank Policy Institute through its technology policy division known as "BITS," the American Bankers Association (ABA), and the Securities Industry and Financial Markets Association (SIFMA) (collectively, the Associations)[1] appreciate the opportunity to comment on the National Institute of Standards and Technology's (NIST) preliminary draft of the Privacy Framework. The Privacy Framework is an important effort that will heighten awareness and help organizations of all sizes better protect sensitive data and improve privacy outcomes for consumers.

I. Executive Summary

The financial services sector is strongly committed to the protection of individuals' data and has long been subject to legal and regulatory requirements to protect the privacy, security, and confidentiality of customer information.[2] We believe the NIST Privacy Framework will help other organizations not subject to similar requirements improve their awareness of privacy risks and implement a governance structure to more effectively manage and communicate the risks inherent in holding and processing consumer data.

In the Associations' previous submission[3], we encouraged NIST to use similar structures identified in the Cybersecurity Framework (CSF); to recognize that domestic and international privacy laws and requirements already exist and create an imperative to harmonize efforts; and to assist in developing clear definitions and a common lexicon.

---

[1] See Annex A for a description of the Associations
[2] For a discussion of the financial sector's legal and regulatory requirements, please see the Associations' letter to NTIA's "Developing the Administration's Approach to Consumer Privacy" https://www.ntia.doc.gov/files/ntia/publications/financial_trades_ntia_comment_letter_nov_8_2019.pdf
[3] See the Associations' letter dated January 14, 2019 https://bpi.com/wp-content/uploads/2019/01/Financial-Trades-NIST-Privacy-Framework-Letter.pdf

We greatly appreciate that the draft Privacy Framework adopts a similar structure to the CSF, using functions, categories and subcategories to allow firms to methodically think through and assess the types of data they possess, how they use data, how data is controlled and protected, and how data use and associated risks are communicated to stakeholders.

The draft Privacy Framework also recognizes that data processing is not a linear, vendor-supplier relationship, but is rather an ecosystem where data may move between organizations in a variety of ways that impact an individual's privacy. These complex relationships are noted in the draft Privacy Framework and highlight the importance of the Communicate function since the ability to share and exchange information and data is critical to sustaining and protecting a vibrant economy.

As NIST continues to refine the draft Privacy Framework, the Associations offer the following recommendations:

1. **Ensure definitions align to common privacy terms.** While there are a variety of definitions in use by laws and regulatory requirements (e.g. the European Union's General Data Protection Regulation and the California Consumer Privacy Act), there are also well-established definitions used by privacy professionals. NIST should seek to use and align its definitions to those privacy terms that are widely used by privacy professionals and agnostic to specific laws and regulations.

2. **Ensure references to ethical decision making appropriately recognize the lack of objective standards.** The draft Privacy Framework notes that it intends to help support "ethical decision-making in product and service design"[4]. Unlike other areas of privacy and security, what is deemed "ethical" varies between individuals, societies, and jurisdictions, can change over time, and is a determination that exists beyond legal obligations. To avoid creating confusion, we recommend these references be removed to better recognize the ambiguity that exists.

3. **Provide a mechanism to help organizations address conflicts of law and demonstrate compliance.** Many large organizations must comply with numerous privacy requirements, each of which may have different definitions and set varying requirements for the treatment and handling of data. It would be very beneficial if the Privacy Framework could help identify best practices or a methodology for a more granular level of analysis that could be used to demonstrate compliance across multiple jurisdictions and privacy regimes.

4. **Clarify intersections with the NIST CSF.** While the Privacy Framework and NIST CSF are intended to be used in conjunction, organizations would benefit from having greater clarity on the intersection between core elements in both frameworks, particularly in the area of breaches, to allow for easier cross-referencing and to promote an effective, integrated framework.

II. Ensure definitions align to common privacy terms.

A variety of definitions exist for common privacy terms such as "personal information" or "data processing." While we appreciate NIST's effort to remain agnostic to any specific law or regulation, the creation of new terms for the same or similar concepts without reference to existing definitions and their

[4] Page 3, *NIST Privacy Framework: Preliminary Draft*

source, may cause confusion and necessitate the need for firms to map the NIST definitions to terms already in use.

The financial services sector has faced this challenge in the cybersecurity arena and has spent countless hours seeking to align legal and regulatory definitions to better demonstrate compliance and adherence to various frameworks (e.g. the NIST CSF) and best practices. As the privacy arena and the legal landscape continue to evolve, it would be helpful for widely used terms[5] to be included and aligned where possible and their sources referenced in the Privacy Framework.

It would also be helpful if the Privacy Framework included further discussion of the relationships between widely used terms and concepts that exist in legal or regulatory frameworks. For instance, a discussion on how the term "disassociability" relates to concepts like deidentification, depersonalization, anonymization, pseudonymization, and aggregation might be beneficial, particularly to organizations that are less mature in their data and privacy risk management efforts or are subject to multiple regulatory regimes and requirements.

Additionally, we recommend that definitions such as that for "cybersecurity incident" be the same between the CSF and the Privacy Framework. Given the overlap and efforts to align the two Frameworks to facilitate their use, there should be a common set of definitions between the two documents.

III. Ensure references to ethical decision making appropriately recognize the lack of objective standards.

While various standards and legal obligations exist for data privacy and data security, there are few, if any, specific requirements for what may constitute the ethical handling of data. As a result, any evaluation of what is ethical is inherently subjective and attempting to determine whether any given use of data is ethical would be fraught with uncertainty. To avoid creating confusion for organizations that may be less mature in their governance and overall treatment of data, we recommend NIST remove this language in the final Privacy Framework.

As an alternative, NIST could adopt the approach taken within the financial sector to refer to the "responsible" use of data. For example, the Office of the Comptroller of the Currency's Office of Innovation has implemented a framework for responsible innovation[6] that seeks to balance new products and services with appropriate risk management to protect customers and the financial institution.

Many large financial institutions have developed governance bodies and procedures to review new uses of data as well as potentially new data sources to ensure they fit with the institution's risk management framework, culture, and values. Although responsible innovation may be a somewhat broader concept, other organizations that are not subject to similar governance and oversight expectations may benefit from a deeper discussion of mechanisms to thoroughly consider data use and its potential effects, including procedures for escalating responsible decision-making regarding these considerations.

---

[5] See International Association of Privacy Professionals Glossary of Privacy Terms https://iapp.org/resources/glossary/#paperwork-reduction-act-2

[6] See Office of the Comptroller of the Currency https://www.occ.treas.gov/topics/supervision-and-examination/responsible-innovation/index-responsible-innovation.html

IV. Provide a mechanism to help organizations address conflicts of law and demonstrate compliance.

In addition to a deeper discussion of how various terms and concepts may interrelate as discussed above, a more detailed discussion of best practices to address conflicts of law and demonstrate compliance would be highly beneficial. Global organizations face competing demands to comply with data localization requirements, specific data security demands, and individual data rights that differ across jurisdictions. Even organizations that are purely U.S- based face growing challenges as additional states consider and enact data privacy and security requirements that are similar but different in terms of how they define key terms and desired outcomes. The challenge of ensuring adherence to different standards and the ability to demonstrate compliance is one that many organizations will struggle with and an area where NIST could develop tools and practices organizations could adopt.

V. Clarify intersections with the NIST CSF.

Given the areas of overlap between privacy and security functions within organizations, the draft Privacy Framework highlights these areas and how the two Frameworks may be used together to manage privacy risks. In particular, we appreciate the addition of the "Govern" function to the draft. The financial services sector has found governance to be critically important to managing both cybersecurity and privacy risks and added a Governance function to our Sector Cybersecurity Profile.[7]

With regard to breaches, the draft Privacy Framework describes the connection to cybersecurity risks in section 1.2.1 and references it in Figure 2. However, stronger cross-references to the relevant aspects of the NIST CSF, particularly in sections 2 and 3 of the draft Privacy Framework, would help drive consistency for organizations to apply a coherent methodology. For example, the Profile development process described in section 2.2 could include linkages to the Core elements of the CSF and should facilitate easier cross-reference to help an organization to have an effective, integrated framework. Recent reviews of breaches by regulators (e.g., Marriott, British Airways) included an assessment of those companies' governance and other aspects of privacy and security risk management, such as record retention processes, to determine the penalties.

* * * * *

We appreciate NIST's efforts to develop the preliminary draft Privacy Framework and the open and transparent dialogue it has fostered regarding improving privacy outcomes for individuals. Modernization and the digitization of our economy have created numerous benefits for individuals, businesses, and society, but we must ensure all organizations take responsibility for managing and protecting individuals' information. We believe that the NIST Privacy Framework can serve as a valuable tool that organizations may use to build and adapt a privacy program that fits the size, complexity, risk profile, and unique attributes of a particular institution and their sector.

Thank you for the opportunity to comment on the preliminary draft. If you have any questions, please contact Heather Hogsett, Senior Vice President for Technology and Risk Strategy, BPI/BITS at Heather.Hogsett@bpi.com or 202.589.1930, Bill Boger, Senior Vice President and Chief Legislative Counsel, ABA at WBoger@aba.com or 202.663.5424, or Melissa MacGregor, Managing Director and Associate General Counsel, SIFMA at MMacGregor@sifma.org or 202.962.7385.

[7] See https://bpi.com/financial-services-sector-cybersecurity-profile/

Annex A

The Bank Policy Institute (BPI) and BITS:

BPI/BITS is a nonpartisan public policy, research and advocacy group, representing the nation's leading banks. Our members include universal banks, regional banks and the major foreign banks doing business in the United States. Collectively, they employ nearly 2 million Americans, make 72% of all loans and nearly half of the nation's small business loans and serve as an engine for financial innovation and economic growth.

The Business-Innovation-Technology-Security division (better known as BITS), is a division of BPI that brings BPI's banks and other affiliate members together in an executive-level forum to discuss and promote current and emerging technology, foster innovation, reduce fraud and improve cybersecurity and risk management practices for the nation's financial sector. For more information, visit http://www.bpi.com.

The American Bankers Association (ABA):

ABA is the voice of the nation's $17 trillion banking industry, which is comprised of small, midsized, regional, and large banks. Together, these institutions employ more than 2 million people, safeguard $13 trillion in deposits and extend more than $9.5 trillion in loans. For more information, visit http://www.aba.com.

The Securities Industry and Financial Markets Association (SIFMA)

SIFMA is the leading trade association for broker-dealers, investment banks and asset managers operating in the U.S. and global capital markets. On behalf of our industry's nearly 1 million employees, we advocate for legislation, regulation and business policy, affecting retail and institutional investors, equity and fixed income markets and related products and services. We serve as an industry coordinating body to promote fair and orderly markets, informed regulatory compliance, and efficient market operations and resiliency. We also provide a forum for industry policy and professional development. SIFMA, with offices in New York and Washington, D.C., is the U.S. regional member of the Global Financial Markets Association (GFMA). For more information, visit http://www.sifma.org.