January 14, 2019

Via Electronic Mail

National Institute of Standards and Technology (NIST)
Docket No. 181101997-8997-01
Request for Information: "Developing a Privacy Framework"

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

Dear Dr. Copan:

The Bank Policy Institute (BPI) 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 provide comments to the National Institute of Standards and Technology (NIST) on its "Request for Information on Developing a Privacy Framework: An Enterprise Risk Management Tool" (RFI).

I. Executive Summary

The NIST effort to create a Privacy Framework (Framework) will help "improve organizations' management of processes for incorporating privacy protections into products and services"[2] across all sectors of the economy and is a critical effort to improve privacy outcomes for consumers and better protect sensitive data. As the Associations noted recently in a submission to the National Telecommunications and Information Administration (NTIA), [3] the financial services sector is strongly committed to the protection of consumer data, privacy, and security. Privacy protections are embedded in the operations and governance structures of financial services firms, in part due to the long-standing and extensive legal and regulatory requirements they must adhere to. Financial firms must comply with comprehensive federal, state and international standards for the management and protection of customers' personal information

1 *See* Annex A to this letter for the descriptions of the Associations
2 *See* NIST Docket No. 181101997-8997-01
3 *See* 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

and have created robust internal data governance structures that focus on risk management and govern the collection, use, control, and transparency of customer data.

The NIST effort is timely and the Associations recommend the following themes for consideration:

1. Use Similar Structures Identified in the Cybersecurity Framework (CSF) to Create a Privacy Framework:

To improve privacy outcomes across all sectors of the economy, NIST should build upon the collaborative effort it started with the private sector to create the Cybersecurity Framework (CSF), which includes a compendium of technical standards and reference materials that organizations can use to better understand, assess, and manage privacy risks. For sectors like financial services, there are a wide array of existing privacy laws, fiduciary duties, and regulations that are both process and outcome focused, and the sector has created practices over the years that are subject to regulatory review and examination to meet these requirements.

2. Help Other Sectors Develop Mature and Robust Frameworks for Managing Privacy Risks:

Similar to the CSF process, the creation of a Framework should leverage the expertise and experience of more mature sectors to help improve privacy outcomes across all sectors of the economy. The Framework will help sectors that are presently subject to minimal privacy requirements to develop more mature and robust frameworks for managing privacy risk. The Framework being developed could include "lessons learned," adaptable practices such as those used in the financial services sector, and a range of technical standards that organizations can utilize if they fit their respective requirements.

For purposes of this filing, the Associations focus on four key components of the RFI:

1. Structuring a Privacy Framework (Framework)
2. Organizational Considerations: Extensive Requirements Already Exist
3. Harmonizing Efforts Around the World
4. Developing Clear Definitions and a Common Lexicon

II. Structuring a Privacy Framework (Framework)

A. The Framework Should Follow a Similar Structure to the CSF

It is important for the NIST process to focus on creating a document similar in structure to the CSF that serves as a tool organizations of varying sizes and maturity can use to better understand how to manage privacy risks in this increasingly data-centric age. The financial services sector already complies with a range of domestic and international privacy and data protection laws, and the Framework process should not directly, or indirectly, create a new, overlapping, or duplicative process. Rather, NIST should focus on creating a Framework that provides overall structure and

self-assessment models to assist organizations in creating governance structures and operational policies to manage privacy risks and demonstrate accountability for remediating those risks.

Privacy and security risks arise in companies of all sizes. An organization's privacy risk profile should be based on the number of individuals whose personal information it collects, processes, and/or shares, as well as the sensitivity of those data, and not on variables with little or no bearing on privacy risk, such as an organization's revenue, size, or total number of employees. As with the CSF, broad-based constructs for understanding and managing privacy risks will help create a level playing field across all sectors and fill in the gaps for sectors with less mature privacy practices. Privacy and security are shared risks and all sectors should meet consistent standards.

In many cases, financial institutions are required by regulators to ensure that any vendors and third party service providers that may have access to customer information adhere to regulatory requirements related to privacy. The creation of any Framework should clearly articulate that third parties that process, pass-through, or store consumer information also have a responsibility to ensure the privacy, security, and proper management of the data they hold in their possession. All entities should implement privacy practices which will provide increased protections for consumers' privacy and security across the board.

As with the CSF, an effective Framework would result in all parties' ability to describe their current privacy practices and objectives; maintain a process to identify and prioritize opportunities for improvement that are continuous and repeatable; and assess progress and communicate effectively among internal and external stakeholders about privacy risk. [4]

The Value of Core Functions and Implementation Tiers

The Framework should also include similar organizational constructs to those in the CSF as a means to help organizations understand how to manage privacy risks. Concepts like the "Core Functions" are easily adaptable to privacy. For example, three of the five main CSF Core Functions – "Identify," "Protect," and "Detect" – are critical functions to manage privacy risk.[5]

Identifying where data are, how sensitive or important they are, how they are held, and how they are used, is critical for all companies.

Properly securing and protecting personal data from unauthorized disclosure is certainly a must and the data must also be protected from potential misuse. Organizations should establish clear data governance structures and be aware of who should and should not have access to certain types of personal data to protect against misuse.[6]

The "Detect" function also can be used for privacy purposes by ensuring there are internal and external structures in place that govern authorization to access personal data and by ensuring that

[4] *See* NIST Cybersecurity Framework 1.1: Framework Introduction
[5] *See* Ibid 2.1 Framework Core
[6] Data, in this context, are not defined to avoid confusion.

data access rights can be revoked as needed. Concepts including "privacy by design," "privacy by default," and even "least privileged access to data" should be fully incorporated throughout the creation of Core Functions.

Other key tools in the CSF such as tier structures (1-4), coordination mechanisms (Executive, Business Process and Implementation/Operations), [7] and seven steps to establishing or improving a cybersecurity program[8] are also adaptable to privacy issues and should be included in a Framework, adjusting terms and explanations to be focused on managing privacy risk and applicable compliance obligations.

B. The Privacy Framework Should Not Be Based on Specific Standards

The RFI asks a series of questions on how best to structure a Privacy Framework including whether it should be structured around specific standards or concepts including "information life cycle, principles such as the Fair Information Practice Principles (FIPPs) and the NISTIR 8062: An Introduction to Privacy Engineering and Risk Management in Federal Systems." Examples such as FIPPS and NISTIR 8062 were all created specifically for the federal government, and while useful as general privacy constructs, there are aspects of each that may not align well with the private sector. Each have different connotations that could add unnecessary complexity and confusion for sectors like financial services that are already subject to a host of existing legal and regulatory requirements that carry their own definitional implications.

Other sectors that are not subject to similar requirements could benefit greatly from having useful standards to look to. To help those sectors improve their ability to manage privacy risk, the Framework should include an Appendix with a variety of standards and requirements that sectors like financial services must meet as examples of effective practices other organizations could consider.

III. Organizational Considerations: Extensive Domestic and International Privacy Laws and Requirements Already Dictate Global Efforts

As NIST is aware, financial services firms have long been subject to federal, state and international standards for the management and protection of customer information. The need to protect customer information and preserve confidentiality and privacy has been deeply embedded in the policies and operations of banks, insurance companies, wealth and asset management firms and other financial service companies for decades.

As the Associations' described in their comments to NTIA,[9] there are multiple legal and regulatory regimes that establish requirements, standards, and expectations for managing privacy risk and handling customer data. These include, but are not limited to the following:

---

7 *See* NIST Cybersecurity Framework Section 2.4
8 *See* Ibid Section 3.2
9 *See* October 26, 2018 Filing before NTIA

- **Gramm-Leach-Bliley Act (GLBA) and the Interagency Guidelines**: The GLBA and its implementing regulations[10] include a detailed and extensive list of requirements around the collection, use and protection of consumer data along with specific privacy and information security requirements, such as the Safeguards Rule. The information security programs of banks, as required by the GLBA, follow the requirements laid out in the prudential regulators' Interagency Guidelines. [11]
- **Federal Financial Institutions Examination Council (FFIEC) Information Technology (IT) Examination Handbook:** The FFIEC IT Examination Handbook is an extensive document and denotes specific areas of compliance covering a wide range of issues including: (1) governance and (2) information security program management, including risk identification, risk measurement, risk mitigation, and risk monitoring and reporting.
- **Right to Financial Privacy Act (RFPA**): The RFPA protects individuals against unwarranted federal access to searches of personal financial records. The RFPA addresses and specifically restricts how financial institutions can share financial records with the government without customer authorization, an administrative subpoena or summons, a valid search warrant, a judicial subpoena, or a formal written request such as a civil investigative demand. [12]
- **State data security and privacy laws**: State laws also govern how the financial services sector uses and protects personally identifiable information. The overlapping and growing patchwork of state laws is creating a complicated, duplicative, and often times conflicting and costly compliance burden for financial institutions. For example, the New York Department of Financial Services' (DFS) new cybersecurity rules[13] impose duplicative and therefore confusing security obligations, and the new California Consumer Privacy Act (CCPA) of 2018 has extensive privacy and consumer data requirements.
- **International data security and privacy laws**: There also are numerous privacy laws globally with which financial institutions must comply. The requirements of privacy laws and regulations outside the United States should be considered in any framework, with an awareness that some laws may conflict with existing U.S. laws around data retention and use for anti-money laundering (AML), sanctions, and law enforcement purposes.

Varying aspects of these and other legal and regulatory requirements dictate what financial institutions must do with personal data when they are received, how long they need to be retained, and how they must be secured, among other things. Some of these requirements include: (1) AML mandates; (2) economic sanctions imposed by Treasury's Office of Foreign Assets Control (OFAC); (3) identity protection, including the Interagency Guidelines on Identity Theft

---

10 Establishing Information Security Standards and the Interagency Guidance on Response Programs for Unauthorized Access to Customer Information and Customer Notification. See https://www.fdic.gov/news/news/financial/2005/fil2705.html

11 *See* Interagency Guidelines 12 C.F.R. Part 30, Appendix B.

12 *See Id*. § 3402.

13 See https://www.dfs.ny.gov/legal/regulations/adoptions/dfsrf500txt.pdf

Detection, Prevention, and Mitigation; and (4) federal reporting requirements including the Home Mortgage Disclosure Act and tax reporting obligations.[14]

It is important to note that while technological change has reshaped and refined the availability and use of data, existing consumer protection and privacy requirements still govern the use of new financial technology (FinTech) applications by financial institutions. For instance, the availability of new technologies to help detect fraud and anomalous behaviors using voice and other biometric tools provide added convenience, security and choice for consumers. Other FinTech innovations use data to help expand access to credit and provide new products to meet the needs of the underserved and unbanked around the world. Based on the sector's long-standing requirements, privacy considerations are embedded into the operations, procedures, and governance structures that financial services companies use when applying new technology. Financial institutions implement, test, and continually update information security and privacy programs that are reviewed by Chief Privacy Officers or compliance staff and executive management as well as the board of directors. These programs are subject to supervision by regulators.

IV. Need for Harmonization Efforts Globally

The Associations support NIST's efforts to create a Framework and to help ensure that all sectors of the economy better manage privacy risks. As the world becomes more reliant on the use of data, all entities and organizations involved in the collection and use of data must be accountable for managing privacy risk. As with the CSF, NIST partnered with other agencies in the U.S. Government to discuss its benefits around the world. It is equally important for NIST to do the same with respect to a Privacy Framework. Other nations have moved quickly to establish privacy structures and requirements and it will be critical for NIST to ensure that the creation of a Privacy Framework can help harmonize efforts globally.

As the Associations noted in the NTIA filing, the Framework process should bring clarity for those operating globally and help set a benchmark for all entities and new entrants into the marketplace that privacy is something all companies must protect. As the technological revolution creates new opportunities and new tools to provide the consumer with more choices and improved service, new market entrants must understand that privacy and security should be part of the fundamental design of any new product or service.

U.S. leadership will be particularly important in preserving an open global economy that enables trade, investment, and growth through the secure and efficient transfer of data across borders. The Framework should discourage unnecessary limitations in the flow or storage of data across international boundaries. The global trend toward data localization, which may include data on-shoring, ring-fencing, or demanding businesses use certain standards or technologies, will limit

[14] It is important to note that the financial services sector is also subject to extensive regular exams by a multitude of regulators who conduct rigorous ongoing oversight of operating and governance practices. Few other sectors are subject to this kind of oversight, which can include substantial restrictions on bank activities and fines if regulators identify any deficiencies.

innovation and impair economic growth. A better approach is to limit changes in regulation related to storage, use, or transfer of data that could have unintended impacts on security and global operations. The development of a Framework that reflects U.S. legal precedent and encourages economic development should balance the following factors:

1) the ability to transmit data across national boundaries and store data in different jurisdictions is fundamental to supporting a secure, innovative, and prosperous global financial system, and fostering global economic growth;
2) the capacity of cross-border data mobility to support information security;
3) the need of industry supervisors to fulfill regulatory obligations across multiple jurisdictions using targeted cross-border information sharing; and
4) the criticality of third-party outsourcing arrangements to improve the efficiency of financial services.

Global structures like the G7, G20, Basel Committee, and the Organization for Economic Cooperation and Development exist to help create broader harmonization efforts. The U.S. should remain vigilant and active in these venues to promote U.S. interests.

V. Need for Clear and Consistent Definitions

Similar to the process used in the CSF to create a "Glossary," the creation of a Framework must avoid using terms that are either too broad or conflict with terms used in existing laws and regulations. Standard terms and definitions in privacy requirements will need to be carefully analyzed, for example, terms including "consumer vs. customer," "personal information" or "personal data," "control," "access and correction" all have specific definitions for the financial services sector.[15] The Associations would be happy to collaborate with NIST on the creation of a common lexicon that is consistent with the existing definitions in the financial services sector.

VI. Next Steps

The Associations believe it is critical that this Framework and any discussion about the use of technical standards and organizational structures account for the existing and effective functioning of the financial system, which currently has the most robust and comprehensive privacy requirements that exist across all industries today. We look forward to contributing to the creation of a Framework and other tools that raise the bar for privacy for all sectors of the

---

[15] *See* 15 U.S.C. § 6809(9)): https://www.gpo.gov/fdsys/pkg/USCODE-2011-title15/html/USCODE-2011-title15-chap94-subchapI-sec6809.htm; 15 U.S.C. § 6809(4) and implementing regulations; 15 U.S.C. § 6809(9)): https://www.gpo.gov/fdsys/pkg/USCODE-2011-title15/html/USCODE-2011-title15-chap94-subchapI-sec6809.htm; *1*5 U.S.C. § 6809(4) and implementing regulations; 16 C.F.R. pt. 313 Subpart A; SB-1121, 2017-2018, California Consumer Privacy Act (Sept. 23, 2018).

economy while preserving the key tenets of privacy protection already adhered to by financial services firms.

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.

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.