November 8, 2018

Via Electronic Mail

National Telecommunications and Information Administration (NTIA)
Docket No. 180821780-8780-01
RIN 0660-XC043
Request for Comments: "Developing the Administration's Approach to Consumer Privacy."

The Honorable David Redl
Assistant Secretary for Communications and Information
National Telecommunications Information Administration (NTIA)
U.S. Department of Commerce
Washington D.C. 20230

Dear Administrator Redl:

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 Telecommunications and Information Administration (NTIA) on its Request for Comments (RFC) on "Developing the Administration's Approach to Consumer Privacy."[2]

I. Executive Summary

Creating a federal privacy framework (Framework) is an important effort to help ensure that consumer data and privacy are protected across all sectors, including those that are not subject to the long-standing and extensive legal and regulatory requirements that have long applied to the financial services sector. The Associations, and the members they represent, are strongly committed to the protection of consumer data, privacy and security and, as a result, support a national effort that can apply appropriate protections across all sectors. As the RFC notes, any new privacy Framework must promote greater trust, transparency and protections for consumers in order to "advance consumer privacy while protecting prosperity and innovation" so that "users… trust that organizations will respect their interests, understand what is happening with their personal data, and decide whether they are comfortable with this exchange."

---

1 *See* Annex A to this letter for the descriptions of the Associations
2 *See* https://www.ntia.doc.gov/files/ntia/publications/fr-rfc-consumer-privacy-09262018.pdf

As NTIA is aware, financial services firms have long been subject to comprehensive federal, state and international standards relating to the privacy and security 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 institutions for decades. Indeed, few other sectors have as extensive or robust a series of legal and regulatory requirements, that together with equally important industry standards, govern the collection, use, control and transparency of customer data. In fact, all seven of the privacy principles articulated by the NTIA in the RFC are already existing cornerstones in the current legal mandates that apply to the financial services industry: (1) transparency; (2) control; (3) reasonable minimization; (4) security; (5) access and correction; (6) risk management and (7) accountability.

Given this robust and well-established regulatory framework already in place for financial institutions, it is important that any voluntary framework developed by NTIA be synergistic with, and not overlapping, inconsistent, or duplicative of the myriad of existing regulatory and legal requirements that the financial services sector already observes and operationalizes on a daily basis. Ultimately, a single, national standard should preempt the current patchwork of state laws to ensure uniformity and provide consumers a clear understanding of their privacy rights.

The following comments are intended to provide (1) contextual information on the legal and regulatory requirements financial services firms must adhere to and are regularly examined against, (2) suggestions on how NTIA should use these extensive requirements as a baseline for a Framework, as well as (3) suggestions on key selected themes in the RFC. The requirements discussed below are just a subset of the existing state, federal and global requirements for financial firms and are intended to help inform how the financial sector should be considered in the development of a Framework.

II. Existing Extensive Privacy Laws and Requirements

The important role that the United States' financial services industry plays in the global economy and in consumers' lives can be traced back to 1791 when the First Bank of the United States was created. Since that time, the industry has seen the evolution of state, federal and international laws and regulations that govern how and what type of consumer data can be collected, used, retained and secured. Even the underlying definition of consumers' personal identifiable information (PII) is defined by statute. The governing structures include but are not limited to:

- The Gramm-Leach-Bliley Act (GLBA) and its implementing regulations
- The Interagency Guidelines Establishing Information Security Standards and the Interagency Guidance on Response Programs for Unauthorized Access to Customer Information and Customer Notification (collectively, the Interagency Guidelines)
- The Fair Credit Reporting Act (FCRA)
- The Federal Financial Institutions Examination Council (FFIEC) Information Technology (IT) Examination Handbook
- The Right to Financial Privacy Act (RFPA)
- State data security and privacy laws

- International data security and privacy laws

Varying aspects of these requirements, and other existing legal and regulatory mandates, dictate what financial institutions must do with the data when they are received as well as how long they need to be retained and secured, among other things. For example, some of these requirements include: (1) anti-money laundering (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 Detection, Prevention, and Mitigation; and (4) federal reporting requirements including the Home Mortgage Disclosures Act and tax reporting obligations.

It is important to note that the financial services sector is also subject to robust regulatory oversight as well as 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 deficiencies.

At the same time, technological change has reshaped and refined the availability and use of data, but these existing requirements still govern the use of financial technology (FinTech) applications which are providing for greater security, usability and flexibility for consumers. 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. As a new voluntary privacy Framework is created, it must be developed in a way that accommodates the technological changes of tomorrow and focuses on desired outcomes rather than specific technologies or methods.

III. Longstanding Privacy and Cybersecurity Efforts

A. Existing Privacy Requirements and Consumer Protections

Data security and the protection of consumer data has long been a cornerstone of the financial services industry's mission and compliance programs. Financial institutions must collect sensitive personal information about customers to help inform safe lending decisions and to comply with robust regulatory requirements. This information is used to help prevent fraud and identity theft, improve the security of customer accounts, and to safely expand access to credit. Preserving the trust of consumers and protecting the integrity and confidentiality of their accounts and data has always been, and will continue to be, of paramount importance to the industry.

In collecting this information, financial institutions invest considerable resources to help ensure it is kept safe, secure and used appropriately. Financial institutions implement, test and continually update information security and privacy programs that are reviewed by senior executives such as Chief Information Security Officers, Chief Privacy Officers and/or compliance staff and executive management as well as the board of directors. These programs are subject to regular examination by regulators. Regulators have a wide latitude to impose fines, restrict activities and increase scrutiny of a firm's overall activities if they identify deficiencies, which are then reassessed and additional penalties and restrictions can be added if deficiencies are not addressed. While there are other sectors that are required to review, assess and test their security postures, few are required to meet

such extensive mandates as the financial services sector. To meet the wide array of state, federal and global data security and cybersecurity requirements, the financial services sector utilizes sophisticated tools and technologies and is a leader in innovative ways to maintain and protect consumer data.

The following is just a brief listing of key requirements and mandates the sector must meet:

1. Gramm Leach-Bliley Act (GLBA)

GLBA and its implementing regulations 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.[3] GLBA requires financial institutions to inform consumers about how data are collected and shared and, in certain circumstances, allows them to opt out of information sharing. The information security programs of banks, as required by GLBA, follow the requirements laid out in the prudential regulators' Interagency Guidelines.[4] Consistent with these Interagency Guidelines and related guidance, banks develop, implement, and maintain administrative, technical, and physical safeguards designed to (a) protect the security and confidentiality of customer records and information; (b) protect against any anticipated threats or hazards to the security or integrity of such records and information; and (c) protect against unauthorized access to or use of such records or information that could result in substantial harm or inconvenience to consumers.[5] Interagency Guidelines also direct financial institutions to provide notice to customers impacted by a security breach under certain circumstances.

It is also worth reiterating that GLBA provides for additional consumer protections, including dictating when customers' information can and cannot be disclosed to nonaffiliated third parties and when financial institutions must provide their customers with the opportunity to opt of sharing with such parties. These provisions provide privacy protections to consumers and ensure that consumers will also be able to benefit from an effective and innovative financial system.

For example, financial institutions are prohibited from disclosing a consumer's nonpublic personal information to a nonaffiliated third party unless: (1) the consumer has received notice and an opportunity to opt out of such sharing and has not opted out; or (2) an exception permitting the disclosure applies, such as to process transactions or maintain or service accounts.[6]

It is critical to note that the exceptions to the right to opt-out are specifically tailored around the types of disclosures that financial institutions must make in order to provide the very financial products and services that consumers want. For instance, in order to process a credit card transaction, a bank must communicate its authorization for the transaction to the relevant payment card network and/or merchant.

---

3 16 C.F.R. Part 314.

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

5 15 U.S.C. § 6801(b); 16 C.F.R. § 314.4(b).

6 Gramm-Leach-Bliley, Section 502 (b)(1).

2. Federal Financial Institutions Examination Council (FFIEC) Interagency Guidelines and IT Examination Handbook

The FFIEC Interagency Guidelines and the IT Examination Handbook is an extensive document that includes various discrete booklets providing an exhaustive list of requirements on various IT-related issues. For example, the Handbook provides regulatory expectations for, among other things, information security, business continuity planning and supervision of technology providers. The Information Security Booklet denotes specific areas of compliance covering a wide range of information security issues including: (1) governance; (2) information security program management, including risk identification, risk measurement, risk mitigation and risk monitoring and reporting; (3) security operations; and (4) information security program effectiveness. [7]

3. Right to Financial Privacy Act (RFPA)

The RFPA[8] protects individuals against unwarranted federal searches of personal financial information. It 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.[9]

4. State Data Security and Privacy Laws

State laws also govern how the financial services sector uses and protects PII. The overlapping and growing patchwork of state laws is creating a complicated, duplicative, and often times conflicting and costly compliance burden for financial institutions. Varying definitions of PII, data breach reporting mandates, timelines and fines also make it difficult at best for any consumer to truly understand how their data are used and protected. The following lists just a few of the existing state requirements:

a. New York Department of Financial Services (DFS): The new DFS Cybersecurity requirements mandate covers financial institutions and requires that they maintain cybersecurity programs and policies, based on the institution's risk assessment, to address data governance, systems and network security and monitoring, customer data privacy, vendor management, and incident response, among other things.[10]

b. Massachusetts Standards for the Protection of Personal Information of Residents of the Commonwealth (Standards): Massachusetts requires minimum standards be met in connection with safeguarding PII to ensure confidentiality, protect against threats or hazards, and protect against unauthorized access.

---

7 *See* FFIEC IT Examination Handbook, IT Booklet, *Information Security* (Sept. 2016), https://ithandbook.ffiec.gov/media/274793/ffiec_itbooklet_informationsecurity.pdf ("Information Security Booklet").

8 *See* 12 U.S.C. §§ 3401-3422.

9 *Id.* § 3402.

10 *See* New York Codes Rules and & Regulations (NYCRR), Title 23, § 500.

c. California Financial Information Privacy Act (CFIPA): CFIPA, which explicitly states that it is intended to provide greater protection than GLBA,[11] prohibits financial institutions from selling, sharing, transferring, or otherwise disclosing "nonpublic personal information" to or with any nonaffiliated party without the explicit consent of the consumer or unless an enumerated exception applies.[12]

d. California Consumer Privacy Act (CCPA) of 2018: CCPA is a sweeping privacy law that includes themes similar to the new European Union (EU) Global Data Protection Regulation (GDPR) and dramatically expands the scope of personal information covered to "information that identifies, relates to, describes, is capable of being associated with, or could reasonably be linked, directly or indirectly, with a particular consumer or household." While it includes an exemption for personal information "collected, processed, sold, or disclosed pursuant to" the GLBA and its implementing regulations or the California Financial Information Privacy Act, the dramatic expansion of the definition of CCPA will have significant impacts on the financial services sector. [13]

e. State Data Disposal Laws: Over half of U.S. states also have laws that require businesses to utilize specific data disposal and/or destruction requirements for digital and/or paper records containing PII.[14]

5. Global Requirements

Financial institutions are also subject to numerous global privacy and data security laws if they operate in other countries or handle a European subject's data under new laws like the EU's GDPR. GDPR dictates new and stringent limitations on collection, use, processing and deletion of personal data related to individuals in the EU.[15] Challenges exist to address compliance issues as some aspects of GDPR may conflict with requirements for use and retention under U.S. law for AML, sanctions, and other U.S. law enforcement related matters. At the same time, other nations around the world including Brazil,[16] Canada[17] and Mexico[18] have either recently passed or had other data protection laws on the books for some time.

---

11 *See* California Financial Code § 4051(b).

12 *Id*. § 4052.5.

13 *See* SB-1121, 2017-2018, California Consumer Privacy Act (Sept. 23, 2018).

14 *See* National Conference of State Legislatures, *Data Disposal Laws* (Dec. 1, 2016), http://www.ncsl.org/research/telecommunications-and-information-technology/data-disposal-laws.aspx.

15 *See* Regulation (E.U.) 2016/679 of the European Parliament and the Council of 27 April 2016 on the Protection of Natural Persons with Regard to the Processing of Personal Data and on the Free Movement of Such Data, and Repealing Directive 95/46/EC (General Data Protection Regulation), 2016 O.J. L 119/1.

16 *See* Brazil: General Data Protection Law: http://www.planalto.gov.br/ccivil03/Ato2015-2018/2018/Lei/L13709.htm

17 *See* Canada: The Personal Information Protection and Electronic Documents Act (PIPEDA): https://www.priv.gc.ca/en/privacy-topics/privacy-laws-in-canada/the-personal-information-protection-and-electronic-documents-act-pipeda/

18 *See* Mexico: General Data Privacy Law, the Lei Geral de Proteção de Dados Pessoais https://www.pnm.adv.br/wp-content/uploads/2018/08/Brazilian-General-Data-Protection-Law.pdf

B. Voluntary Cybersecurity Practices

Privacy cannot be provided without robust security measures to protect data and prevent the unauthorized use or disclosure of consumers' information. The financial services industry also has a myriad of legal and regulatory cybersecurity requirements that require extensive compliance and places a great importance on cybersecurity issues. To support that focus, the industry has invested in and adopted voluntary practices above and beyond what is required. In many cases, the industry has led the way in demonstrating the effectiveness of efforts that are increasingly being used around the world.

The following are just a few examples of these efforts:

1. National Institute of Standards and Technology (NIST) Cybersecurity Framework

The industry was among the first to adopt the voluntary NIST Cybersecurity Framework and has embarked on an ambitious effort to map the Cybersecurity Framework to the underlying financial services sector cyber requirements. Partnering with NIST, through the Financial Services Sector Coordinating Council (FSSCC), [19] the financial sector has created an industry specific set of guidelines for cybersecurity programs known as the Financial Sector Cybersecurity Profile.[20]

2. Financial Services Information Sharing and Analysis Center (FS-ISAC)

The FS-ISAC is one of the longest operating ISACs and reflects the industry's belief in the importance of voluntary information sharing on cyber risks across the sector. Both the U.S. Departments of the Treasury and Homeland Security, including the United States Computer Emergency Readiness Team (U.S.CERT), use the FS-ISAC to disseminate critical security information to the financial services sector, and financial institutions work collaboratively with public and private sector partners to identify and share cyber and physical threat intelligence to help prevent data loss or corruption through early warning systems. [21]

3. Committee on Payments and Market Infrastructures (CPMI) – International Organization of Securities Commissions (IOSCO)

The financial services sector also spends an extensive amount of time working on best practices for cybersecurity around the world and believes in the importance of making sure that global efforts are as seamless as possible.[22] Collaborations such as those through the CPMI IOSCO around guidance on cyber resilience for financial market infrastructure continue and are providing key practices around the world.

---

19 *See* Financial Services Sector Coordinating Council, https://www.fsscc.org/About-FSSCC.

20 *See* https://bpi.com/financial-services-sector-cybersecurity-profile/; www.aba.com/cyberprofile; https://www.fsscc.org/Financial-Sector-Cybersecurity-Profile

21 *See* FS-ISAC: https://www.fsisac.com/

22 *See* IOSCO: Guidance on Cyber Resilience for Financial Market Infrastructures: https://www.bis.org/cpmi/publ/d146.pdf

4. Payment Card Industry (PCI) Data Security Standard (DSS)

The financial services sector has also instituted self-regulatory efforts that include compliance with the PCI-DSS, specific standards the industry uses for protecting cardholder data.[23] It applies to entities that store, process, or transmit cardholder data and/or sensitive card-related authentication data (such as "track data," CVVs, or PINs). PCI-DSS also includes 12 different requirements covering the encryption of cardholder data in transmission, developing and maintaining secure systems and applications, tracking and monitoring access to network resources and cardholder data, and regularly testing security systems and processes.[24]

IV. Need for Harmonization Efforts in the U.S. and Around the World

The Associations strongly support efforts to promote appropriate privacy frameworks and to bring other sectors of the economy up to the mature requirements adhered to by the financial sector. However, any new efforts should focus on federal preemption of the multitude of state laws and ensure harmonization with existing, and any future, global requirements. This will bring clarity for those operating globally and help set a benchmark for all new entrants into the marketplace that privacy is something all companies must protect. As the technological revolution is creating new opportunities in the marketplace, as well as 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.

At the same time, nations around the globe are debating and mandating new hybrid laws that integrate varying aspects of privacy laws, cybersecurity requirements and data localization concerns. It is critical that NTIA work with NIST, the International Trade Administration (ITA), the U.S. Department of State, and all of the various offices within the White House to ensure that the voluntary frameworks that are being created here in the U.S. are part of these global discussions. Where there are large-scale shifts in global policy, the U.S. needs to be at the forefront to provide U.S. companies with clarity and a level playing field.

Global structures like the G7, G20 and 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. Third Party Providers

Privacy and cybersecurity should be shared responsibilities, and it is critical that vendors and third party service providers meet consistent standards. In many cases, the regulatory burden is placed on financial institutions that are in turn generally mandated to impose requirements on vendors and third parties, and financial institutions can become responsible for third parties' compliance with these requirements.

---

[23] *See* PCI Security Standards Council, *Payment Card Industry (PCI) Data Security Standard: Requirements and Security Assessment Procedures* v.3.2.1 (May 2018), https://www.pcisecuritystandards.org/documents/PCI_DSS_v3-2-1.pdf

[24] *Id*. at 19-115.

The creation of any Framework should clearly articulate that third parties who may process, pass-through, or store consumer information also have a responsibility to protect it. Encouraging all entities to implement adequate privacy practices will provide for increased protections for consumers' privacy and security.

In one particular instance, the RFC seems to indicate that the relative size of the company, the amount of data collected, and similar factors[25] should determine whether or not a company should be required to meet privacy or security mandates. It is important for NTIA, in the creation of the Framework, to avoid the impression that any of these issues should be determinant of whether or not privacy or security is important. As an example, organizations should not necessarily be measured by revenue or number of employees, but by the number of individuals whose personal information it collects, processes, and shares, as well as the sensitivity of that data.

VI. Need for Consistency on Definitions

The RFC requests comments on how key terms should be defined. As described above, the financial services sector already has a myriad of legal definitions it uses to operationalize privacy requirements. It is important for the NTIA process to ensure that any definitions in the Framework do not conflict with existing sectoral, state, and global requirements. At the same time, there are a host of other sectors that do not have GLBA-like requirements and have no clear definitions that must be met. To that end, it is important to understand how NTIA plans to address issues around key definitions and for that process to be fully open and transparent. This is especially important for those sectors that already have definitions like this in well-established bodies of law.

Within the scope of the seven principles articulated by NTIA, it is critical that there be a seamless and transparent process to address what the definitions mean and ensure consistency with existing law. There are certain definitions used by NTIA that are defined differently by GLBA, as well as a host of other laws that already have conflicting and duplicative approaches. For example:

1. **"Consumer vs. Customer:"** Definitions vary greatly and need to be streamlined to define a foundational term like consumer or customer. GLBA distinguishes between these terms: a consumer is "an individual who obtains, from a financial institution, financial products or services which are to be used primarily for personal, family, or household purposes, and also means the legal representative of such an individual." A "customer" is a consumer who has a "customer relationship" with a financial institution. A "customer relationship" is a continuing relationship between a consumer and a financial institution under which the institution provides one or more financial products or services to the consumer that are to be used primarily for personal, family, or household purposes.[26]

2. **"Personal Information:"** There are a multitude of overlapping and confusing definitions of personal information and personally identifiable information (PII) across federal, state, local, and international laws. Under GLBA, the term that is used is "nonpublic personal

[25] *See* NTIA RFC Section B(8) "Scalability"

[26] *See* 15 U.S.C. § 6809(9)): https://www.gpo.gov/fdsys/pkg/USCODE-2011-title15/html/USCODE-2011-title15-chap94-subchapI-sec6809.htm

information" i.e., "personally identifiable financial information" that a financial institution collects about a consumer in connection with providing a financial product or service.[27]

- CCPA adds definitions of personal information that are exceptionally broad and include categories such as commercial information (e.g., records of products or services purchased, obtained or considered), and other consuming histories or tendencies; internet activity (e.g., browsing and search history and interactions with advertisements); and data drawn from personal information to create profiles reflecting consumer preferences and attitudes.
- State data breach laws also include an array of differing, overlapping and conflicting definitions of PII and are increasingly adding varying forms of biometrics into these definitions as well.

3. **"Control," "Access and Correction**:**"** The concepts of "Control" as well as "Access and Correction" are important to consider but it is also critical to understand that they are foundational issues that are defined under GLBA. For a host of other sectors, none of these terms are defined in law and attempting to create a Framework that conflicts with GLBA is not an acceptable situation for the financial sector.

   - GLBA addresses how nonpublic personal information about consumers can be handled as this letter has discussed in an earlier section, including certain prohibitions on disclosing this information to third parties, specific opt-out provisions, as well as how consumers/customers may access and correct their data.[28]
   - In the case of GDPR, requirements around control, access and correction are exceptionally prescriptive and require institutions to make major changes internally to allow for these concepts and those that go even farther, such as the right to erasure. Yet in many cases, these requirements conflict with existing U.S. laws around AML and data retention matters.
   - In the case of CCPA, it adds a host of new layers within these concepts by providing California consumers the right to request a detailed listing of how their personal information is collected and where it came from, how it is sold and disclosed, and to whom it is disclosed or sold.[29]

4. **Accountability**: Accountability is also a critical concept to the financial services sector and is addressed throughout the GLBA, FCRA and other privacy rules the financial services sector is required to meet. As NTIA creates this Framework, this is also a critical term that should be applied to other sectors as well.

---

27 *See* 15 U.S.C. § 6809(4) and implementing regulations.

28 *See* 16 C.F.R. pt. 313 Subpart A

29 *See* SB-1121, 2017-2018, California Consumer Privacy Act (Sept. 23, 2018).

For instance, the Framework must ensure that all sectors have a structure that provides equal accountability across the board, including third party providers. Certainly, the rise of Internet of Things (IoT) devices has demonstrated that concepts of "privacy by design" and "security by design" need to be embedded in devices at the front end, integrating a culture of shared responsibility by all. The effort by the U.S. Departments of Commerce and Homeland Security to address risks around botnets and malware, as required by Executive Order 13800, and included in the May 2018 "Report to the President on Enhancing the Resilience of the Internet and Communications Ecosystem Against Botnets and Other Automated, Distributed Threats" highlighted the need for shared risk and shared responsibilities across the ecosystem.[30]

VII. Clarification on Overall Process

As indicated, the Associations appreciate the overall process that NTIA is convening but seek clarification on how the NTIA process and the efforts by NIST to create a Privacy Framework will be coordinated. Both agencies are working on important privacy missions, however, many of the same questions and issues are being addressed in different venues and it is not yet clear how they may go together to create an overarching federal privacy policy framework. At the same time, the financial services sector is already subject to substantial regulatory oversight on these issues. As a result, the RFC raises a number of important policy and procedural questions that the Associations believe are important to address and resolve prior to the finalization of any Framework, including:

1. Will NTIA review and utilize GLBA and Interagency privacy regulations as a basis for this effort?
2. How will NTIA and NIST create a structure that is not duplicative or conflicting with existing legal requirements? How will the NTIA and NIST processes address sectors like financial services that are already heavily regulated for privacy?
3. How will the NTIA and NIST processes be coordinated to avoid two different privacy frameworks?
4. What are the venues that will allow the private sector to continue to participate? Is there a timeline and plan that can be shared with industry to better understand how these processes will be working together?
5. How will the NTIA Privacy Framework effort be reviewed to ensure there is no overlap or duplication with the NIST Cybersecurity Framework as well as the NIST Risk Management Framework?
6. How are NIST, NTIA, ITA and the U.S. Department of State working together to address the global proliferation of privacy laws and their impact on U.S. companies?

VII. Next Steps

The RFC states that the Administration would like to be able to determine the "best path toward protecting individual's privacy while fostering innovation." As articulated in the RFC, a desired outcome is "a reasonably informed user, empowered to meaningfully express privacy preferences"

[30] *See*: https://www.commerce.gov/page/report-president-enhancing-resilience-against-botnets

along with products and services that are inherently designed to protect privacy, particularly in situations where "user intervention may be insufficient to manage privacy risks." [31]

From the perspective of the financial services industry, it is critical that this or any other proposed outcome be considered in the context of the existing and well-founded standards, and effective functioning of the financial system which currently has the most robust, comprehensive, and stringent privacy requirements that exist across all industries today. We look forward to developing a national standard for privacy that is consolidated, coherent, and consistent with current laws and requirements the financial services community is already subject to.

We appreciate this opportunity to provide comments on this RFC and would welcome the opportunity to discuss our comments with the NTIA and the Administration further. 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.

[31] *See*: https://www.ntia.doc.gov/files/ntia/publications/fr-rfc-consumer-privacy-09262018.pdf

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.