Ms. Katie MacFarland
National Institute of Standards and Technology
100 Bureau Drive, Stop 2000
Gaithersburg, MD 20899

VIA EMAIL: privacyframework@nist.gov

RE: Developing a Privacy Framework - Docket Number 181101997–8997–01

IBM appreciates the opportunity to respond to National Institute of Standards and Technology's (NIST) Request for Information on Developing a Privacy Framework as part of the United States approach to addressing global privacy concerns. We welcome the government-industry collaboration to address privacy risk faced by organizations, governments and citizens alike. IBM has repeatedly stated that a stakeholder engagement to identify privacy best practices, guidance, technical controls, and any gaps that may exist will better inform any comprehensive national law to address privacy issues in the United States.[1]

As IBM's long history of security and privacy leadership demonstrates, IBM understands that protecting privacy is essential to trust. IBM was one of the first companies to appoint a Chief Privacy Officer,[2] to develop and publish a genetics privacy policy,[3] to be certified[4] under the APEC Cross Borders Privacy Rules system,[5] and to sign the EU Data Protection Code of Conduct for Cloud Service Providers.[6]

We look forward to this engagement with NIST and the final product of this important exercise that ultimately will impact how organizations and government handle personal data, protect individuals and support privacy.

Data is the phenomenon of our time. It is the world's new natural resource, growing exponentially not only in quantity but more importantly in form. Every action and interaction, every decision and relationship, every event occurring in any of the world's complex systems, natural and human-made, is now being expressed as data. This data is already fundamental and central to many commercial business models and industries. As a global technology company that is constantly innovating in new technologies, we believe we have a clear responsibility in our handling of data, and to lead in the privacy and protection of that data. Data requires clarity around the principles and rules of the road to ensure that it is not misused and that it is adequately protected. IBM defined and communicated the following key areas of policy in our Trust and Transparency Principles[7] to illustrate our commitment to protecting data and ensure trust for our clients in handling data.

- Clients are not required to relinquish rights to their data to have the benefits of IBM's Watson AI solutions and services
- We believe the unique insights derived from clients' data are their competitive advantage, and we will not share them without their agreement
- IBM client agreements are transparent. We will not use client data unless they agree to such use and we will limit that use to the specific purposes clearly described in the agreement
- IBM employs industry-leading security practices to safeguard data. This includes use of encryption, access control methodologies, and proprietary consent management modules which allow us to restrict access to authorized users

[1] https://www.ibm.com/blogs/policy/ntia-consumer-privacy
https://www.ibm.com/blogs/policy/american-approach-data-privacy
[2] https://www.ibm.com/press/us/en/pressrelease/1464.wss
[3] https://www.ibm.com/ibm/history/ibm100/us/en/icons/geneticprivacy/
[4] https://www.ibm.com/press/us/en/pressrelease/41760.wss
[5] http://www.cbprs.org/
[6] https://www.ibm.com/blogs/policy/eu-cloud-code-of-conduct/
[7] https://www.ibm.com/blogs/policy/trust-principles

As we embark upon developing a framework for privacy, it is important to reflect upon what "framework" meant from the NIST Cybersecurity Framework development process – "a language and structure for risk management processes that will be implemented differently in each organization, not a checklist of specific measures that must be taken or outcomes that must be achieved."[8] Building upon the successful model of the NIST Cybersecurity Framework, there are themes from that engagement that also are applicable to this exercise for developing a privacy framework:

- Voluntary and flexible - Recognize different industries have differing approaches and future needs, where a one-size fits all approach risks leaving organizations without the latest innovations and potentially making them less secure;
- Risk-based management approach - Recognize that total risk elimination is often impossible, a process of risk management allows for identification, prioritization, and reasonable remediation of risk to individuals and organizations;
- Technology-neutral – Does not prescribe or mandate the use of specific technologies, measures or tools;
- International standards - Leverage existing global standards and industry best practices to enable interoperability and foster development of new standards to fill an identified gap;
- Education – Ongoing awareness and education of risks and current best practices for individuals, organizations, practitioners, regulators and priority stakeholders

Again, we applaud NIST for recognizing the need to instantiate a risk management approach as the foundation of this privacy framework to enable organizations to identify, assess, and manage their risk - analogous, and potentially, complementary to the Cybersecurity Framework. We offer in this response high-level observations on the importance of trust and accountability, flexibility and innovation, risk management programs and leveraging industry standards as they relate to the topics probed in the RFI.

Trust & Accountability

Trust and accountability are the cornerstone of any privacy framework. In order for organizations (large and small) to deliver on the myriad of varied data privacy and cybersecurity obligations around the world, and to exceed the ever increasing market demands for transparency, they must incorporate trust and accountability as core guiding principles into the very fabric of the organization's culture and processes.

Trust and accountability are founded on transparency. Without transparency, organizations cannot build and maintain trusted relationships. Accountability requires a trusted, transparent and documented organizational structure comprised of policies, processes, practices, controls and above all common values that guide strategic and business objectives. Transparency is critical. Accountability also requires transparency with consumers. Ensuring transparency through strong organizational policies around data and building capabilities, wherever possible, to set preferences or choices for data use, are crucial steps to fostering trust and confidence.

Accountability means a system that places responsibility for protecting consumer data and privacy on organizations collecting or handling consumer data, particularly in an information society and ecosystem that is complex and continuously evolving. Organizational accountability embodies the following core elements[9]: risk-assessment, policies and procedures (taking into consideration fairness and ethics), transparency, training and awareness, monitoring and verification, response and enforcement, and leadership and oversight. A privacy framework should incorporate these elements as the foundation to how an organization approaches privacy.

Organizations can draw upon existing tools and organizational structures to build out these core elements as part of a privacy accountability system. Organizations also can participate in globally recognized and well established programs designed to verify and certify accountability mechanisms

[8] http://csrc.nist.gov/cyberframework/preliminary_framework_comments.html - IBM response to NIST Preliminary Cybersecurity Framework, December 2013

[9] http://www.informationpolicycentre.com/uploads/5/7/1/0/57104281/cipl_accountability_paper_1_-_the_case_for_accountability_-_how_it_enables_effective_data_protection_and_trust_in_the_digital_society.pdf

such as APEC Cross-Border Privacy Rules (CBPR), APEC Privacy Recognition for Processors (PRP), and national privacy marks like Japan's JIPDEC Privacy Mark System. Also available are frameworks such as the EU Binding Corporate Rules (BCR) and EU-US Privacy Shield. We encourage NIST to consider these existing programs when developing a privacy framework.

Finally, organizational commitment to Security and Privacy by Design ("SPbD") is fundamental to trust and accountability. SPbD requires that the key principles of data minimization, privacy by default, adequate security, and accountability are considered at the outset, and not as an afterthought, to the development of products and services. SPbD plays a significant role in driving best practices as early as possible into the development process. By considering privacy and security throughout the lifecycle of a product or service, organizations can assure continuous improvement of their security and privacy practices and ongoing alignment with evolving global privacy frameworks and compliance models. IBM encourages NIST to consider the importance of Security and Privacy by Design in an overall privacy framework.

Establishing accountability systems helps protect consumers, gives them confidence that their data will be handled appropriately, and builds trust with consumers, regulators, and business partners. In addition, if properly designed, such systems also help organizations adapt quickly to challenges presented by evolving and disparate regulatory requirements. An effective privacy framework should include ways in which to improve accountability through development of standards and best practices and also build recognition by consumers and regulators that adoption of the framework meets the fundamental privacy protections.

Principle-based Flexibility & Enable Innovation

Flexibility, is a critical feature of an effective privacy framework. A flexible, principles-based framework helps an organization continuously address and improve the management of privacy risk arising from collection, storage, use, and sharing of consumers' personal information. We appreciate NIST's intention for the "Framework to provide a prioritized, flexible, risk-based, outcome-based, and cost-effective approach that can be compatible with existing legal and regulatory regimes".[10]

Flexibility means that companies and other organizations building privacy into their accountability systems are given the freedom, in the context of their existing systems, to determine how best to meet all privacy criteria, whether established in law, by self-regulation or through application of best practices.

This attribute of flexibility provides a number of benefits for consumers, businesses, and the U.S. economy. First, more and more organizations now interact with and manage data, and this phenomenon is rapidly expanding. A one-size-fits-all, prescriptive approach is unworkable across the breadth of the U.S. economy, and across the world. Flexibility in implementation, especially based on best practices and standards developed in a bottom-up, collaborative process – as proposed by NIST's process – is a valuable tool for facilitating widespread adoption of privacy protections. Second, evolving privacy regimes around the world, including the European Union General Data Protection Regulation, are focused on the principles of transparency and accountability. A framework that is grounded in these global principles, but which provides flexibility in implementation, will facilitate interoperability and global implementation of protections of consumer data.

Third, providing flexibility on how to implement will accommodate the development of emerging technologies. Overly prescriptive requirements can result in unforeseen impediments to the development of new technologies that could benefit consumers and, in fact, strengthen consumer privacy protections.

Last, an adaptable, dynamic system for protecting consumer privacy that also fosters innovation will preserve America's competitive advantage in emerging technologies. IBM has long recognized the power data holds for our clients. Therefore, the Framework must be designed to take into account its

[10] Department of Commerce, National Institute of Standards and Technology, Developing a Privacy Framework, [Docket Number 181101997–8997–01], Privacy Framework Development and Attributes

effect on emerging technologies and the impact on U.S. competitiveness, while achieving greater protections for U.S. consumers.

Risk Based Approach & Risk Management Methodology

IBM supports a risk-based privacy framework. A risk-based approach gives organizations the flexibility to address evolving threats to data security and privacy and to identify and accommodate any new risks raised by emerging technologies. This inherently will lead to enhanced data protection. Further, implementing a comprehensive, privacy risk-based management approach is a transformative process that can well-position an organization to leverage its skills, processes, policies and technology to help meet both current and future privacy regulatory obligations.

An effective risk-based framework must be founded on a common understanding of what constitutes a privacy risk and baseline standards for risk mitigation. For example, organizations should take into account the sensitivity of the personal information, the context of its collection and use, and the risk of tangible harm if it is misused. A national privacy framework should provide a common approach to privacy risk management – how to identify, assess and mitigate privacy risk --- without prescribing specific risk-based practices. Establishing a common and consistent privacy risk management methodology will contribute to harmonized practices, further data protection, and advance global interoperability. IBM commends NIST's risk-based approach and encourages NIST to continue to work with stakeholders to establish standards on privacy risk management. Finally, the framework should promote the integration of privacy into existing industry standards for risk management, and encourage the incorporation of privacy into existing enterprise risk management programs and processes.

A framework built on existing standards will facilitate the ability of organizations to leverage their institutionalized risk management practices to adequately assess and address privacy risk. The ISO31000 Standard for Risk Management could provide guidance on the principles, framework and process for overall enterprise risk management in this area. This standard provides for the identification, analysis, evaluation, treatment, ongoing monitoring, and governance of risks. Examples of how to integrate privacy into this existing risk management framework include:

- Establish accountability and management oversight for privacy risk management
- Engage in appropriately broad range of expertise internally and externally
- Identify key privacy risks within the context of the organization, including the threats and consequences
- Analyze and assess risks, determine the potential impact, probability, existing controls, and ability and complexity to mitigate such risk
- Determine the appropriate risk mitigation for each risk, such as reduce the impact, reduce the probability, avoid the risk, share the risk
- Monitor and report on the risk to ensure risk mitigation is effective

Integrating privacy into existing risk management standards will allow organizations to leverage their existing risk management programs to address privacy risks. IBM encourages NIST to work with stakeholders to develop common definitions of privacy risk levels and impacts, and a common approach to assessing and mitigating risk associated with data use.

Leveraging Industry Standards

IBM supports a privacy framework that builds on and enhances existing security and privacy standards and practices and furthers global interoperability of privacy regimes. One of the challenges that organizations face today is a lack of consistency on data protection practices and requirements around the world. Not only will common standards enhance data protection for individuals, but they also will provide organizations with more certainty on best practices for protecting personal data. Mapping the framework to existing standards and requirements would greatly benefit organizations that base their practices on those standards and requirements. A privacy framework that is easily integrated with what organizations already do today is inherently useful and more likely to be accepted and adopted. Moreover, leveraging existing standards and requirements furthers the goal of global interoperability of the framework. A standard that aims for global interoperability is becoming increasingly important, particularly in light of the evolving global privacy regulatory landscape.

As our long history of privacy leadership shows, IBM understands that security and privacy are essential for trust in the global digital economy. IBM was one of the first adopters of the EU Cloud Code of Conduct, a public-private collaboration involving industry, the European Commission, and Data Protection authorities. The Code of Conduct is a valuable tool available to assure cloud users that their data is secure and protected. Similarly, the NIST Cybersecurity Framework, ISO/IEC 27001 standard for information security management and ISO/IEC 27002 Code of Practice for Information Security Controls provide reliable industry standards for data security. A privacy framework should incorporate and build on existing standards such as these in order to achieve the shared goals of enhanced data protection and adoptability of the framework.

A privacy framework also should reflect and support evolving industry standards in the area of privacy. One such example is privacy by design. Regulators, industry, and consumer groups are advocating privacy by design as an essential element to data protection and efforts are underway to develop common standards for privacy by design. The NIST framework should be a “living structure” that accommodates, supports, and fosters the improvement of existing standards and the development of new standards to further protect data privacy for consumers.

IBM would like to again thank NIST for its continued commitment to working with the private sector on critical issues important to the global digital economy and enabling cross sector collaboration and transparency in addressing and finding solutions to current and future challenges. We appreciate the opportunity to provide this input into the beginning of the process to develop a Privacy Framework and look forward to understanding the results of this RFI and exploring many of these topics in more detail with NIST and others at future workshops this year.