From: Marc Williams <marcwill@us.ibm.com>
Sent: Wednesday, October 23, 2019 2:49 PM
To: privacyframework <privacyframework@nist.gov>
Subject: IBM's Comments on the Preliminary Draft of the NIST Privacy Framework

Ms. MacFarland,

Attached are IBM's comments on the National Institute of Standards and Technology's (NIST) Preliminary Draft of the NIST Privacy Framework: A Tool for Improving Privacy through Enterprise Risk Management. We appreciate having the opportunity to comment.

Best regards.

Marc Williams

(See attached file: IBM_Comments_NIST_Privacy_Framework_Preliminary_Draft_October 23, 2019.pdf)

(See attached file: NIST_Privacy_Framework_IBM_Feedback_October 23, 2019.pdf)

Marc Williams
Government and Regulatory Affairs Executive, Intellectual Property
IBM Corporation
600 14th Street, N.W., Suite 300
Washington, D.C. 20005
Tel: 202-551-9382 (tie-line 729)
Fax: 202-551-9691
Internet: marcwill@us.ibm.com

1 North Castle Drive
Armonk, NY 10504
Phone: 914-765-7241

October 23, 2019

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

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

Dear Ms. MacFarland;

IBM appreciates the opportunity to comment on the National Institute of Standards and Technology's (NIST) Preliminary Draft of the NIST Privacy Framework: A Tool for Improving Privacy through Enterprise Risk Management ("the Privacy Framework"). IBM has a long history of security and privacy leadership and responsible stewardship of new technologies based on our Trust and Transparency Principles. We strongly support the Privacy Framework and its final publication later this year.

The Privacy Framework is a valuable tool for organizations of all types and sizes to systemically improve privacy protections for individuals in the United States and beyond. Further, its risk- and outcome-based approach provides flexibility to meet diverse privacy needs while enabling technological innovations in areas such as artificial intelligence and the Internet of Things.

We believe that this Privacy Framework will inform any comprehensive national law to strengthen privacy protections in the United States. It is an important step towards making those protections a reality and should give the public greater confidence that industry now has an effective enterprise risk management tool to enhance consumer privacy in the digital age.

Notably, the Privacy Framework:

- Builds consumer trust by driving robust organizational accountability. The Privacy Framework creates a structured approach to assessing and implementing protections for individuals' data that drives accountability throughout the organization, from the senior management level down to the operational and engineering level.
- Makes it easier and more desirable for organizations to implement privacy protections. The Privacy Framework uses the same structure as the successful NIST Cybersecurity Framework, and is flexibly designed to enable organizations to integrate into existing operational controls, including product and business development operations.
- Is interoperable with global standards, which facilitates compliance and responsible data management across an organization's enterprise, and advances privacy protected cross border data flows, which is critical for our global digital economy.

1 North Castle Drive
Armonk, NY 10504
Phone: 914-765-7241

With a view towards continuous improvement, we are attaching additional specific comments for your consideration.

IBM commends the NIST Privacy Framework team for its dedication to what was a truly collaborative framework development process, with participation by a wide variety of stakeholders and receptivity to public feedback. We look forward to the final publication of the Privacy Framework and plan to promote its adoption.

Sincerely,

Christina Montgomery
Vice President & Chief Privacy Officer

IBM Feedback on the NIST Privacy Framework Preliminary Draft
October 23, 2019

Comment #	Section	Comment (Include rationale for comment)	Suggested Change
1		The International Organization for Standardization (ISO) and the International Electrotechnical Commission (IEC) released ISO/IEC 27701 on August 6, 2019. This new standard is a privacy extension to ISO/IEC 27001 and ISO/IEC 27002, and was developed to help organizations protect and control the personal information they handle, and to continue to improve their Privacy Information Management Systems. IBM recommends including ISO/IEC 27701 in the Privacy Framework's references and encourages NIST to facilitate an authoritative mapping of the Privacy Framework to the new international standard.	
2		Consider adding a subcategory immediately following "ID.IM-P1: Systems/products/services that process data are inventoried."	New subcategory: "Nature and context of the data is identified, and data is classified appropriately. "

IBM Feedback on the NIST Privacy Framework Preliminary Draft
October 23, 2019

Comment #	Section	Comment (Include rationale for comment)	Suggested Change
3	ID.IM-P2: Owners or operators (e.g., the organization or third parties such as service providers, partners, customers, and developers) and their roles with respect to the systems/products/services and components (e.g., internal or external) that process data are inventoried.	Replace the word "inventoried" for "identified".	ID.IM-P2: Owners or operators (e.g., the organization or third parties such as service providers, partners, customers, and developers) and their roles with respect to the systems/products/services and components (e.g., internal or external) that process data are identified.
4	ID.RA-P5: Risk responses are identified, prioritized, and implemented.	It is not very clear what "Risk Responses" means in this section. For newer practitioners or readers less familiar with these practices, it may be helpful to reference the Risk Approaches described in 1.2.2 of the Framework. Also note that this seems better suited to the "Risk Management" category than the "Risk Assessment" one.	
5	ID.DE-P1: Data processing ecosystem risk management processes are identified, established, assessed, managed, and agreed to by organizational stakeholders.	Consider providing examples of "risk management processes".	

IBM Feedback on the NIST Privacy Framework Preliminary Draft
October 23, 2019

Comment #	Section	Comment (Include rationale for comment)	Suggested Change
6	ID.DE-P2: Data processing ecosystem parties (e.g., service providers, customers, partners, product manufacturers, application developers) are identified, prioritized, and assessed using a privacy risk assessment process.	This activity might be better suited for the "Risk Assessment" category.	
7	ID.DE-P4: Interoperability frameworks or similar multi-party approaches are used to manage data processing ecosystem privacy risks.	A discussion around what "interoperability frameworks" are could be useful.	
8	ID.DE-P5: Data processing ecosystem parties are routinely assessed using audits, test results, or other forms of evaluations to confirm they are meeting their contractual or framework obligations.	Third-party audit attestations are commonly used and should be explicitly referenced. The intent here should be that organizations use means available to them commensurate with their risk assessment. Some may take SOC 2 reports, some may want on-site audits. Clarity that these are all acceptable options will reduce cost for all parties involved.	ID.DE-P5: Data processing ecosystem parties are routinely assessed using audits, test results, third party certifications or other forms of evaluations commensurate with risk assessment to confirm they are meeting their contractual or framework obligations.
9	CT.DM-P7: Metadata containing processing permissions and related data values are transmitted with data elements.	This seems like a very specific technical requirement at odds with the flexibility called for by the Privacy Framework.	CT.DM-P7: Processing permissions and related data values are established for data elements.

IBM Feedback on the NIST Privacy Framework Preliminary Draft
October 23, 2019

Comment #	Section	Comment (Include rationale for comment)	Suggested Change
10	CT.DP-P1: Data are processed in an unobservable or unlinkable manner (e.g., data actions take place on local devices, privacy-preserving cryptography).	The first example provided ("data actions take place on local devices") does not illustrate the sub-category adequately. In addition, perhaps it would be appropriate to specifically refer to anonymzation and aggregation if this is the intent of this sub-category.	CT.DP-P1: Data are processed in an unobservable or unlinkable manner (e.g., data actions take place on individuals' devices, privacy-preserving cryptography, anonymzation and aggregation).
11	CT.DP-P3: Data are processed to restrict the formulation of inferences about individuals' behavior or activities (e.g., data processing is decentralized, distributed architectures).	The subcategory should consider both architectures and practices. The suggested change adds examples of data handling practices.	CT.DP-P3: Data are processed to restrict the formulation of inferences about individuals' behavior or activities (e.g., data processing is decentralized, distributed architectures, anonymzation and aggregation).
12	CM.AW-P7: Impacted individuals and organizations are notified about privacy breach or event.	Before notification can take place, there is a need to assess whether notification is required/desirable. As a result, we suggest modifying CM.AW-P7.	CM.AW-P7: Mechanisms are in place to determine whether notification to impacted individuals and organizations in the event of a privacy breach or event is desirable/required.
13		A new subcategory should be added immediately following CM.AW-P7, pertaining to the need to have a mechanism to notify in the event an organization comes to the conclusion it is desirable/required.	Mechanisms are in place to notify impacted individuals and organizations in the event of a privacy breach or event.

IBM Feedback on the NIST Privacy Framework Preliminary Draft
October 23, 2019

Comment #	Section	Comment (Include rationale for comment)	Suggested Change
14	CM.AW-P8: Individuals are provided with mitigation mechanisms to address impacts to individuals that arise from data processing.	Examples are necessary for clarity.	Consider adding "consent withdrawl, data deletion" as examples.
15	PR.DP-P5: Protection processes are improved.	Too vague.	
16	PR.DP-P6: Effectiveness of protection technologies is shared.	It seems that this subcategory should discuss whether the protection technologies are adequate as opposed to whether their effectiveness "is shared", which seems like an unusal criteria as this kind of information is highly sensitive.	PR.DP-P6: Effectiveness or protection technologies are tested.
17		It is important to ensure that all IT and other assets belonging to an organization and containing data are returned by staff or any other party so that data within can be appropriately managed (e.g., deleted).	Consider adding the following subcategory: "PR.DP-P11: Assets are returned upon termination of a relationship."