From: Jordanna <jchord@gmail.com>
Sent: Thursday, October 24, 2019 12:40 PM
To: privacyframework <privacyframework@nist.gov>
Subject: NIST Privacy Framework: Comments

Please see the attached document in response to the Call for Public Comment on the Preliminary draft of NIST Privacy Framework.

Please let me know if there are any questions or follow up I can assist with.

Regards,

Jordanna Chord

Comment #	Page #	Line #	Section	Comment (Include rationale for comment)	Suggested Change	Type of Comment (General/Editorial/Technical)	
1	3	88-92	Executive Summary	The way it's worded here makes it sounds like one can achieve privacy by building customer trust. However, "building customer trust" is more of a benefit of the privacy framework. Suggest moving of words to make it clearer.	1) Starting at line 89, add **"and build customer trust"** 2) At line 90, remove **"Building customer trust by"** (since it's moved up into Line 89) 3) Split remaining first bullet into two: **"- Supporting ethical decision-making in product and service design;** **- Building deployments that optimize beneficial uses of data while minimizing adverse consequences for individuals' privacy and society as a whole;"**	Editorial	
2	4	141	1.0 Privacy Framework Introduction	The document lacks clarity where sometimes it mentions privacy of businesses or privacy of individual people and its not consistent regarding this. Using "Entity" would consistently capture all parties impacted by privacy incidents, regardless of whether they are individual humans, businesses, or collections of people.	**Modify:** "affect individuals" **To:** "affect individuals **or other entities** "	Technical	
3	5	176	1.1 Overview of Privacy Framework	A privacy incident is an event that leads to a potential violation of an organization's privacy profile and could put sensitive data at risk. "Incident" is a broad term that includes many different kinds of events. A privacy breach is a type of privacy incident. All privacy breaches are privacy incidents, but not all privacy incidents are privacy breaches."	**Modify**: ".... organizations manage privacy risks associated with privacy **breaches**." **To**: ".... organizations manage privacy risks associated with privacy **incidents**."	Technical	
4	6	Figure 2	1.2.1 Cybersecurity and Privacy Risk Management and others.	A privacy breach is too specific to apply to all types of privacy issues that might arise. "Incident" is a broad term that can include many different kinds of events. A privacy breach is a specific type of privacy incident. All privacy breaches are privacy incidents, but not all privacy incidents are privacy breaches.	**Modify**: Privacy Breach **To**: Privacy Incident	Technical/General	
5	Entire Document	*	*	See comment for 4.	Replace all instances of "privacy breach" with "privacy incident".	General	
6	7	241-242	1.2.1Cybersecurity and Privacy Risk Management	It seems the whole doc assumes only individuals are subjects of privacy issues, whereas privacy includes businesses/orgs (e. g. sensitive data collected from a business customer and mishandled).	**Modify:** "**Individuals,** whether singly or in groups (including at a societal level) experience the direct impact of problems." **To:** "**Individuals,businesses/organizations** whether singly or in groups (including at a societal level) experience the direct impact of problems."	Technical	

7	7	254-275	1.2.2 Relationship Between Privacy Risk Management and Risk Assessment	This document should not be used to establish yet another risk management framework or risk assessment methodology. Instead make it explicitly clear that other, existing risk management frameworks should be leveraged and limit this document to a high-level description of why risk management is important in the overall context of establishing a privacy framework. Please see comment 8 for suggested replacement content.	**Delete the following content from lines 254-275 :** "....against the risks and to determine the appropriate response. ~~(see Appendix D for more guidance on the operational aspects of privacy risk assessment). Organizations may choose to respond to privacy risk in different ways, depending on the potential impact to individuals and resulting impacts to organizations. Approaches include:~~ ~~Mitigating the risk (e.g., organizations may be able to apply technical and/or policy measures to the systems, products, or services that minimize the risk to an acceptable degree);~~ ~~Transferring or sharing the risk (e.g., contracts are a means of sharing or transferring risk to other organizations, privacy notices and consent mechanisms are a means of sharing risk with individuals);~~ ~~Avoiding the risk (e.g., organizations may determine that the risks outweigh the benefits, and forego or terminate the data processing); or~~ ~~Accepting the risk (e.g., organizations may determine that problems for individuals are minimal or unlikely to occur, therefore the benefits outweigh the risks, and it is not necessary to invest resources in mitigation).~~ ~~Privacy risk assessments are particularly important because, as noted above, privacy is a condition that safeguards multiple values. The methods for safeguarding these values may differ, and moreover, may be in tension with each other. For instance, if the organization is trying to achieve privacy by limiting observation, this may lead to implementing measures such as distributed data architectures or privacy-enhancing cryptographic techniques that hide data even from the organization. If the organization is also trying to enable individual control, the measures could conflict. For example, if an individual requests access to data, the organization may not be able to produce the data if the data has been distributed or encrypted in ways the organization cannot access.~~	Technical	
8	8	278-284	1.2.2 Relationship Between Privacy Risk Management and Risk Assessment	This document should not be used to establish yet another risk management framework or risk assessment methodology. Instead make it explicitly clear that other, existing risk management frameworks should be leveraged and limit this document to a high-level description of why risk management is important in the overall context of establishing a privacy framework. Refer to the NIST Privacy Risk Assessment Methodology (PRAM): https://www.nist.gov/itl/applied-cybersecurity/privacy-engineering/collaboration-space/browse/risk-assessment-tools	**Delete lines 278-284 and replace with the following text:** Organizations may choose to leverage any of several existing risk management and assessment frameworks and standards, e.g. NIST IR 8062, NIST SP 800-30, NIST SP 800-37, ISO 27701, ISO 31000, etc. (see the NIST Privacy Risk Assessment Methodology for more guidance on the operational aspects of privacy risk assessment).	Technical	
9	9	307-309	2.1 Core	The existing wording talks only about communication within an organization. The proposed wording talks about communication in general. The privacy taxonomy is helpful within an organization. It should also be helpful when an organization communicates its policy to customers, users, etc.	**Modify:** "The Core provides a set of activities and outcomes that **enable an organizational dialogue about managing privacy risk."** **To: "**The Core provides a set of activities and outcomes that **can be used to improve the privacy posture of an organization. It allows for clear communication both internally and externally by creating a standard vocabulary with which an organization can discuss current and target privacy profiles.**"	Technical	
10	10	339	2.1 Core	It seems the whole doc assumes only individuals are subjects of privacy issues, whereas privacy of businesses/orgs (e.g. sensitive data collected from a business customer and mishandled).	**Modify:** Develop the organizational understanding to manage privacy risk for **individuals** arising from data processing. **To:** Develop the organizational understanding to manage privacy risk for **individuals /organizations** arising from data processing.	Technical	
11	10	355	2.1 Core	The addition of organization policy clarifies that governance needs to monitor and review policy, so that it can more clearly contrast with the "monitoring and review for incidents" that must occur during protect/execution. See comment 12 for the related addition.	**Modify:** "...Strategy, and **"**Monitoring and **Review".** **To:** **"**....Strategy, and "Monitoring and **Review of Organization Policy"**	Technical	

12	10	372 -373	2.1 Core	Reviewing and monitoring of incidents was mentioned in Figure 6 under Implementation/Operations level, but not here in the summary. It should be added.	**Add text:** **Modify:** .....“Authentication, and Access Control”, “Data Security,” and “Protective Technology.” **To:** .... “Authentication, and Access Control”, “Data Security,”,“Protective Technology” and **"Monitor and review for incidents".**	Technical	
13	13	469	3.2 Strengthening Accountability	The emphasis here is on pre-emptive reporting, but this suggestion extends accountability to ensure that reporting can happen across all organizational levels. This is another opportunity to creating an emphasis on a privacy first culture within organizations.	**Add bolded text:** **Modify: "**respond appropriately." **To:** "respond appropriately. **Across these organizational levels, having an established and safe process for any personnel to identify and report incidents or unforeseen issue can help strengthen the communication and collaboration. Adopting a safe reporting and incident process can also incorporate concepts like a blameless postmortem analysis where the goal is to identify the root business or operational causes and identify resolutions to improve overall privacy posture."**	Technical	
14	13	471	Figure 6 - Implementation / Operation Level	It's important to ensure that when incidents occure they are correctly reported and that those incidents influence the review and update of processes across all organizational levels to prevent future repeated incidents. It is not just the responsibility of a single level.	**Add bolded text:** **Modify:** "Privacy posture, changes in risk, and implementation progress **"** **To:** "Privacy posture, changes in risk, implementation progress **, incident management monitoring and review"**	Technical	
15	14	484-485	3.3 Establishing and Improving Privacy Program	Adding "and individuals" helps to clarify that understanding the relationship/role of the company with respect to users (and users' privacy expectations) is also an important part of effective privacy risk management	**Modify: ".....**its role or relationship to other organizations in the ecosystem" **To:**".....its role or relationship to other organizations **and individuals** in the ecosystem"	Technical	
16	19	664 - 670	Appendix A : Privacy Framework Core	Detect, Respond, and Recover can apply to more than just the privacy breach aspect of privacy risk.	**Modify**: "Because Detect, Respond, and Recover are cybersecurity incident-related, these Functions are greyed out in Table 1 because they are not part of the Privacy Framework, although organizations can find them in the Cybersecurity Framework and use them to further support the management of the **privacy breach aspect of privacy risk.** " **To**: " Because Detect, Respond, and Recover are cybersecurity incident-related, these Functions are greyed out in Table 1 because they are not directly part of the Privacy Framework, although organizations can find them in the Cybersecurity Framework and use them to further support the management of the **privacy risk. "**	Technical	
17	19	671	Appendix A : Privacy Framework Core	There needs to be an emphasis on how privacy incidents can differs from cyber security incidents. Because not all privacy incidents are caused by cybersecurity issues, aka some privacy incidents are due to product or business decisions it's important the institutions consider Protect/Detect/Respond/Recover cover privacy incidents not caused by security issues. Organizations could choose to have similar processes for the two, but some cases may need different activities to resolve the incident.	**Add new bullet just below Figure 8:** Not all privacy incidents are privacy breaches. The framework for Cybersecurity (Detect, Respond, Recover) may not apply to all privacy incidents. It is important that a privacy incident reporting and management process be established to deal with the broader set of privacy issues that may arise. Privacy issues may not be the result of a gap or anomaly from what is stored in the PROFILE but could require a reassessment of the privacy posture and evaluation of business, product, services, processes and operations. For example, a company could find an issue with how they are collecting or displaying data to individuals that is not a clear gap in implementation, but requires re-evaluation the business or operational processes. By involving all levels of the organization in the incident reporting and response efforts, this can instill a privacy forward culture and awareness that can improve the protection of individual and entity privacy.	Technical	
18	21	682	Table 2	Data mapping should include how long data is to be retained, as privacy risk is influenced by the duration data is stored.	**Add a new element in the subcategory after the current ID.IM-P8:** ID.IM-P9 - The expected and actual retention of data (e.g. minimum amount of time data is required to be stored).	Technical	
19	21	682	Table 2 (ID.IM-P3)	Suggest Wording change for ID.IM-P3. As previously suggested, privacy incidents impact more than just individual people so we suggest adding organization.	**Modify:** “individuals” **To:** “organizations/individuals”	Editorial	
20	21	682	Table 2 (ID.IM-P3)	Data maps should consider the applicable regulations that apply to the entities being mapped, and this is often determined by the jurisdiction of those entities.	**Add bullet after ID.IM-P3 and renumber it as ID.IM-P4** : Jurisdiction of organization/individuals (e. g. specific countries, regions, or applicable regulations) whose data are being processed and inventoried.	Technical	

21	21	682	Table 2 (ID.IM-P9)	Privacy risk is influenced by who can access data, so access should be included in the inventory map.	**Add a bullet after ID.IM-P9 and renumber it as ID.IM-P10:** Inventory of individuals, systems and entities who have access to data being inventoried.	Technical	
22	24	682	Table 2 (CT.PO-P5)	Incident response is a large part of managing privacy risk, and there should be controls for handling it.	**Add new item CT.PO-P5:** Policies, processes and procedures for responsibilities for the identification, reporting, and evaluation of privacy incidents.	Technical	
23	25	682	Table 2 (CT.DM-P8)	A stale data access policy can lead to incidents, so a regular review of privileges reduces risk for entities accessing data they no longer have a business need for. These could be evaluated on a schedule (quarterly, annually, etc) or based on other events such as when an employee changes their job function.	**Add new item CT.DM-P9:** Permission to access data elements by individuals is reevaluated on a regular basis or other event such as role change or when the access is used. Access is revoked if it is no longer needed.	Technical	
24	26	682	Table 2 (CM.AW-P7)	A privacy incident is an event that leads to a potential violation of an organization’s privacy profile and could put sensitive data at risk. "Incident" is a broad term that includes many different kinds of events. A privacy breach is a type of privacy incident. All privacy breaches are privacy incidents, but not all privacy incidents are privacy breaches. We recommend replacing "privacy breach" with "privacy incident" in most places to better encompass the events this document should apply to.	**Modify CM.AW-P7:** “privacy breach” to “privacy incident”	Technical	
25	28	685	Table 2 (PR.MA-P2)	Leverages lessons learned from post mortems evaluations back to the maintenance of the policies and procedures. It's not enough to document the incidents, it's important that organizations use them to mitigate future incidents, following up on the suggested changes. Building a post mortem process as part of a privacy framework assures that problems are remedied and mistakes are learned from.	**Add a new bullet under PR-MA-P2 and number it as PR-MA-P3 (new):** Maintenance and repair of controls and protections influenced by the post mortem analysis of privacy incidents	Technical	
26	30	N/A	Appendix B: Glossary	Using "privacy incident" may require a definition so one is being suggested.	**Add a new definition under Privacy Breach:** **Privacy Incident:** A privacy incident is an event that leads to a potential violation of an organization’s privacy profile and could put sensitive data at risk.	Technical	