From: Snyder, Julie N. <jsnyder@mitre.org>
Sent: Tuesday, November 26, 2019 10:04 PM
To: privacyframework <privacyframework@nist.gov>
Subject: NIST Privacy Framework: Preliminary Draft Comments

Dear Privacy Framework team,

Thank you for your tireless work and collaboration across the widely varied stakeholder community to craft the Privacy Framework. MITRE has spent two decades working in privacy risk management and engineering. Between this experience and having seen firsthand the benefits of implementing the Cybersecurity Framework we are excited to see this new privacy risk management resource develop! Attached, please find our comments on the preliminary draft. These have been publicly released through MITRE and can be shared however you see fit. Please let me know if you have any questions.

Best regards,

Julie

MITRE

Julie Snyder, CIPP/G/US, CIPM, CIPT

Principal, NCF Privacy Domain Capability Area Lead

jsnyder@mitre.org

202.491.1500

MITRE National Cybersecurity FFRDC (NCF)

Privacy Engineering @ MITRE

Cybersecurity @ MITRE

Comment #	Organization Name	Submitted By (Name/Email)	Page #	Line #	Section	Comment (Include rationale for comment)	Suggested Change	Type of Comment (General/Editorial/Technical)
1	MITRE	Julie McEwen/jmcewen@mitre.org	N/A	N/A	N/A	The document as written is pretty neutral regarding the terminology that it uses. However, this could make it difficult for readers, especially those who work in the privacy field who typically use terminology provided in various Fair Information Practice Principles (FIPPs) frameworks, to relate to the concepts provided.	Consider providing a mapping between concepts used in this document and key concepts in FIPPs frameworks that are commonly used (e.g., OECD guidelines) to provide a frame of reference for those working in the privacy area who are used to the terminology used in FIPPs frameworks.	General
2	MITRE	Julie Snyder/jsnyder@mitre.org	3	88-92	ecutive Summ	Some of the phrasing of the benefits is difficult to digest (e.g., wordy in spots) and consumes the more compelling overall points (e.g., building trust).	Suggest rephrasing the sentence and bullets beginning on line 85 as follows: "The Privacy Framework can build trust, drive better privacy engineering, and help organizations protect individuals' privacy by: • Supporting ethical decision-making in products and services, which optimizes beneficial uses of data while minimizing adverse privacy consequences for individuals and society as a whole; "	Editorial
3	MITRE	Ehijelle E. Olumese (eolumese@mite.org)	3	93	Executive Summary	An emphasis on being proactive regarding future-proofing should be added in order to more directly encourage organizations to actively stay abreast of anticipated changes to technologies and regulations.	Suggest editing the bullet that begins on line 93 to read as follows: Fulfilling current compliance obligations, as well as proactively future-proofing products and services to meet these obligations in a changing technological and policy environment;	Editorial
4	MITRE	Julie Snyder/jsnyder@mitre.org	3	97-99	Executive Summary	The house-building analogy is a useful one but it took a few re-reads to understand how it was being applied.	Suggest rephrasing the analogy on lines 97-99 as follows: Like building a house, where homeowners trust that the foundation is well-engineered enough that they can feel comfortable focusing on choosing between room layouts, effective privacy risk mitigations that are already engineered into products and services provide a foundation for individuals to make choices regarding available privacy protections.	Editorial
5	MITRE	Julie Snyder/jsnyder@mitre.org	3	109-110	Executive Summary	For the reader that doesn't make it past the Executive Summary, it would be helpful for them to understand that the Privacy Framework enables dialogue both internally and externally.	Suggest noting the internal and external impact of the dialogue enabled by the Core in the bullet on lines 109-110 as follows: "The Core enables a dialogue internally and externally..."	Editorial

6	MITRE	Julie Snyder/jsnyder@mitre.org	4	146-152	Executive Summary	The last set of bullet points in the Executive Summary make important points, but for readability would benefit from a lead in sentence and consistent phrasing that makes it clearer how they align.	Recommend adding a sentence before the bullets at the end of line 146 and slightly adjusting the bullet phrasing as follow: "This openness comes through: • Remaining flexible regarding the different parts of an organization's workforce, including executives, legal, and information technology (IT), that may take responsibility for different outcomes and activities. • Encouraging cross-organization collaboration to develop Profiles and achieve outcomes. • Providing usable outcomes for any organization or entity regardless of its role in the data processing ecosystem—the complex and interconnected relationships among entities involved in creating or deploying systems, products, or services."	Editorial
7	MITRE	Ehijelle E. Olumese (eolumese@mite.org)	5	175	1.1 Overview of Privacy Framework	Since this is the first time "data processing" is used substantively in the document and is critical in understanding the Privacy Framework, a brief definition of the term should be added directly to the text. At first glance, one may not understand data processing to include data collection.	Consider adjusting the sentence that begins at the end of line 175 to read: "The first four can be used to manage privacy risks arising from data processing (i.e., any of the collective set of data actions that may occur throughout the data life cycle), while Protect-P can help organizations manage privacy risks associated with privacy breaches."	Technical

8	MITRE	Julie Snyder/jsnyder@mitre.org	5	184-185	1.1 Overview of Privacy Framework	Unless there is a show-stopping desire from industry to include language regarding organizations adding or creating their own Functions, Categories, and Subcategories, the Privacy Framework should stay silent on this similar to the Cybersecurity Framework. Once individual organizations start creating their own versions of the Privacy Framework Core, the Privacy Framework starts losing utility as a communication tool externally because organizations are once again speaking multiple privacy dialects or even languages. This doesn't mean organizations can't supplement the Privacy Framework with additional activities they find useful or that NIST should openly discourage customizing the framework, but encouraging individual versions invites confusion until consensus edits can be made to future versions of the Privacy Framework.	Suggest removing the sentence that reads, "The organization can create or add Functions, Categories, and Subcategories as needed," as well as related references throughout (e.g., Section 2.2 @ line 380-1, Section 3.1 @ line 446-7, Section 3.3 @ line 499-500). Suggest instead using Profiles as the ideal location for discussing the unique needs of the organization. If NIST really wants to encourage organizations to customize the Privacy Framework, then recommend including discussion regarding the pros and cons of doing so (e.g., Pro: Your organizations articulates its needs with greater specificity, Con: Your partners and vendors may not have the policies, procedures, etc., in place to achieve those outcomes, and may even decline to follow them since they are not part of the consensus/NIST version of the Privacy Framework) and organizations should be encouraged to share those changes with NIST for consideration for future versions of the framework.	Technical

9	MITRE	Ehijelle E. Olumese (eolumese@mite.org)	8	265-266	1.2.1 Cybersecurity and Privacy Risk Management	These sentences assume that all organizations will only choose to accept risk because they are minimal or unlikely to occur. However, an organization's risk appetite may just be high due to the nature of their business causing them to accept the risk regardless of its likelihood of occurring. This scenario should be mentioned here or at some point.	Consider addressing the organizations that may have a high risk appetite and encouraging them to include priavacy as a priority.	General
10	MITRE	Ehijelle E. Olumese (eolumese@mite.org)	8	275-277	1.2.1 Cybersecurity and Privacy Risk Management	Adding commas makes the statement @ lines 275-277 clearer.	Consider adjusting the sentence that begins on line 275 as follows: "Privacy risk assessments can help an organization understand, in a given context, the values to protect, the methods to employ, and the way to balance implementation of different types of measures."	Editorial
11	MITRE	Ehijelle E. Olumese (eolumese@mite.org)	8	279-281	1.2.1 Cybersecurity and Privacy Risk Management	Adding a word or phrase that speaks to anticipating proper responses to future/anticipated privacy issues/"problems" will help drive this portion home for executives and members of the legal community utilizing this document.	Consider adjusting the sentence that begins on line 279 to read: "Identifying if data processing could create problems for individuals, even when an organization may be fully compliant with applicable laws or regulations, can help with staying ahead of the regulatory curve and ethical decision-making in system, product, and service design or deployment.	Technical
12	MITRE	Ehijelle E. Olumese (eolumese@mite.org)	10	341-342	2.1 Core	Although the activities in the Identify-P Function are indeed foundational for effective use of the Privacy Framework, I would go further to suggest that they are most critical for effective use of the Privacy Framework. Without truly grasping this part of the framework, the remaining effort will be flawed.	Consider adjusting the sentence that begins on line 341 to read: "The activities in the Identify-P Function are foundational and critical for effective use of the Privacy Framework."	Technical

13	MITRE	Julie Snyder/jsnyder@mitre.org	10	374-384	2.2 Profiles	Aligning strategic direction of business requirements with privacy outcomes should be the purpose of the Profiles, which is consistent with the Cybersecurity Framework as written and in practice. A business requirement (which has evolved to "mission objective" in a number of CSF implementations based on early direction from NIST) could encompass any combination of values, priorities, and other items listed. For organizations that already have Cybersecurity Framework Profiles, making it clear that the Privacy Framework Profiles can be similarly aligned to business requirements/mission objectives will make it easier to use both frameworks together (e.g., adding Subcategories from the Privacy Framework where they enable mission objectives/business requirements already included in an organization's Target Profile).	Consider suggesting orienting Profiles around business requirements, using the other inputs to inform how they are articulated and the elements prioritized from the Core.	Technical
14	MITRE	Julie McEwen/jmcewen@mitre.org	11	404	2.3	The document states that the Tiers do not represent maturity levels. However, the terms used to describe them are similar to those used in several well-known Maturity Models. This could be confusing to readers.	Recommend identifying other terms to use to describe the different Tiers that will not be so closely associated with Maturity Models.	Technical
15	MITRE	Julie Snyder/jsnyder@mitre.org	18	632	Appendix A	Under the Note to Users, Item 3 references Profiles and talks about a Profile including a Category. The Profiles description in Section 2.2 talks about Current and Target Profiles as indicating "outcomes," and Subcategories are described in Section 2.1 as "outcomes," which effectively means Profiles align priorities with Subcategories. This is consistent with the CSF in its descriptions of Subcategories and Profiles, as well as how many are applying CSF Profiles, but the example here suggests a Profile can be articulated at the Category level. Categories aren't specific enough to lend to "outcomes." Should we assume that pointing to a Category simply means all Subcategories in the Category apply in a Profile?	Recommend adding language that clarifies whether this example is intended to include all Subcategories in a Category if that is the intent, or clarifying what is meant by aligning to a Category in a Privacy Framework Profile.	Technical

16	MITRE	Julie McEwen/jmcewen@mitre.org	23	GV.MT-P	Monitoring and Review	Threat identification is an important part of privacy continuous monitoring, and is not mentioned in the document.	Recommend adding privacy threats to GV.MT-P1 as follows: GV.MT-P1: Privacy risk is re-evaluated on an ongoing basis and as key factors, including the organization's business environment, *identified privacy threats,* governance (e.g., legal obligations, risk tolerance), data processing, and systems/products/services change.	Technical
17	MITRE	Julie Snyder/jsnyder@mitre.org	25	CT.DP-P6	Disassociated Processing	Subcategory CT.DP-P6 reads as generally about limiting processing, and not specific to outcomes related to disassociability that CT.DP suggests. This is an expected practice in many domains even when disassociability is not an objective. The outcome is an important one, but seems broader than this Category like a better fit in Data Management.	Consider moving this Subcategory to Data Management.	Technical
18	MITRE	Julie McEwen/jmcewen@mitre.org	30	687	Appendix B	Privacy risk is defined as the likelihood that individuals will experience problems resulting from data processing and the impact should they occur. This definition is too broad and does not reflect the unique nature of privacy in that privacy is specifically related to the control of information about individuals.	Consider changing the "privacy risk" text so that it reads: Privacy risk can be understood as the likelihood that individuals will experience problems resulting from processing information about them and the impact should problems occur.	Technical
19	MITRE	Julie Snyder/jsnyder@mitre.org	33	733-738	Appendix D	The enterprise risk management strategy includes language stating that the process will "likely require tradeoffs." While this is true, we know privacy tends to be an easy loser in those conversations. Along with that, Privacy by Design, which is called for in GDPR, aims to adjust this thinking with it's positive-sum principle. In the scope of a privacy document, the trade-off language here in Appendix D may inadvertently imply privacy is one of the things that should be traded. Examples of what those trade-offs may be would be helpful to those that are new to the discussions.	Recommend adding an example immediately following this sentence: "Limitations on resources to achieve mission/business objectives and to manage a broad portfolio of risks will likely require trade-offs." The example may say something like: "Examples of trade-offs include adjusting the schedule to address a new privacy requirement so that there is greater trust in a service provided to individuals, re-allocating budgetary resources applied to automate a privacy control to increase effectiveness, delaying spending on a tool to address lower privacy risks and relying on policies and procedures until more resources are available, incorporating privacy evaluation criteria into business partner and tool selection processes."	Technical

20	MITRE	Julie Snyder/jsnyder@mitre.org	33	739	Appendix D	Additional Subcategories may also help with this activity: - ID.IM-P3 will clarify the nature of the stakeholders that are individuals, which can aid in understanding the types of privacy outcomes and concerns that apply to the systems/products/services - ID.IM-P8 and ID.RA-P1 will help identify stakeholders based on what the systems/products/services are doing.	Consider adding ID.IM-P3, ID.IM-P8, ID.RA-P1 as related Subcategories.	Technical
21	MITRE	Julie Snyder/jsnyder@mitre.org	41	954-949	Appendix F	Drafts of the Cybersecurity Framework that were made available for review included the roadmap content, but this section remains incomplete in the preliminary draft of the Privacy Framework. Deciding the topics that are addressed in v1.0 and those that will remain for future work and updates in later drafts is a critical decision.	Consider providing the draft of the roadmap for review and comment prior to finalizing V1.0 to increase collaboration and industry buy-in.	Technical