From: Jennifer Reichle DiDonato <reichle.jennifer@gmail.com>
Sent: Thursday, October 24, 2019 3:26 PM
To: privacyframework <privacyframework@nist.gov>
Subject: NIST Privacy Framework Comments

Hello,

Per the request for comments, here are the comments we had on the NIST Privacy Framework.

Please let me know if you have any questions.

Regards,

Jennifer Reichle DiDonato

#	Submitted By (Name/Email)	Page #	Line #	Section	Comment (Include rationale for comment)	Suggested Change	Type of Comment (General/Editorial /Technical)
1	Jennifer DiDonato/ Christine Eaton	9	300	2	There needs to be some sort of explanation showing the integration of the 3 components: Core, Profile, Tier. Currently they are outlined, but there is nothing showing how they work together.	It appears that the suggestion is that the profiles are helpful to create a current state profile and a target state profile. You can work through the Cores to develop the current state profile. Then you can work through the Cores to determine your targeted state profile.	General
2	Jennifer DiDonato/ Christine Eaton	9	306	2.1	There should be an additional Function: Respond. A large part of privacy, as evidenced through multiple regulations, is the ability and requirement to respond during an Incident. The document refers to these as cybersecurity incidents, which is partially correct. But anytime you have an incident involving loss of data concerning an individual, that is a privacy incident. While the organization may have specific cyber requirements there, it can also have or be required to have specific timing requirements, disclosures, etc as required by privacy legislation. One of the more prevalent requirements in the US by statue is on data breach notifications for privacy. This should be a separate function that can reach back to the Cybersecurity Framework.	Additional Function: Respond	Technical
3	Jennifer DiDonato/ Christine Eaton	9	306	2.1	There should be an additional Function: Reassess. Currently this framework appears to be a one time practice, then compliance. However, organizations are changing, technology is changing, risk appetites based upon fines and cases change, and the regulatory landscape is continually changing. Part of a privacy framework is keeping up with those changes through an annual review and reassessment of the phases. Sometimes it may be going back through and saying nothing has changed, but that hasn't been happening and I doubt this will stop changing any time soon. By adding the Reassess function you are showing the need to go back through, to identify changes, new regulations, technologies, missions, and corporate endeavors and are making sure that those identified changes are being incorporated throughout the framework.	Additional Function: Reassess	Technical
4	Jennifer DiDonato/ Christine Eaton	11	405	2.3	The tiers look like Maturity models, but it states that it isn't. The function of the tiers is mirroring that of a maturity model. The guidance within the document regarding the tiers also mimics that of a maturity model. However, it explicitly states it is not a maturity model. If you're going to explain that, it should show how it isn't a maturity model. Just because it may only make sense for an organization to reach tier 2 doesn't mean it isn't a maturity model. It just means the risk may not necessitate the investment to move to a tier 3 or 4.	Remove the statement that it isn't a maturity model. Maybe even just move to the Privacy Maturity Model AICPA or CICA	Technical
5	Jennifer DiDonato/ Christine Eaton	12	434	3.1-3.6	I found these sections to be very confusing, as did my peers. I think the idea was how to use the privacy framework in conjunction with other currently operating processes within a corporation. However, it was very high level without any actual use cases, some sections I couldn't find a tie back, and I don't think any of it was very instructive. I think Section 3.0 outlines that you can use it as needed within your organization and it should be left at that. Otherwise, it should be broken down into the specifics of how you actually apply the framework.	Remove Sections 3.1-3.6	General
6	Jennifer DiDonato/ Christine Eaton	21	Table 2	ID.IM-P6	In addition to data elements it should have the applicable regulations and the data subject intake location. What I mean by that is lately regulations are covering data based on where the data is captured (GDPR Physically located EU/EEA, CCPA California residents when in CA, etc) If it is PI, where the person was located at the time of capture is increasingly important to be able to determine if it is regulated.	Applicable Regulations & Data Intake Location	Technical

7	Jennifer DiDonato/ Christine Eaton	23	Table 2	GV.AT.P	This is an area that most organizations fail to do effectively. I'd love to see additional guidance here to include frequency and suggestions on more role-based training.	At least annual training	Technical
8	Jennifer DiDonato/ Christine Eaton	24	Table 2	CT.PO-P2	This section is missing Data Retention requirements. Each organization should determine data retention periods for each type of data dictated by business need and regulatory requirements.	Add data retention here.	Technical
9	Jennifer DiDonato/ Christine Eaton	24 & 25	Table 2	CT.DM-P3-P5	This should be phrased that specific data elements can be accessed/deleted/disclosed across all platforms. A big problem is complying with customer requests to remove data when data may be stored in separate systems across the organization. Having a way to access data elements and do so across all platforms.	across all platforms and systems within an organization	Technical
10	Jennifer DiDonato/ Christine Eaton	25	Table 2	CT.CP-P	This does not seem like a category in control, but more like a subcategory. Additionally Privacy by Design should be a category in Control. Privacy by Design is the gold standard in Privacy compliance essentially stating that it is embedded into the design of systems, processes, and organizations. It is the top control of any privacy framework. A subcategory of Privacy by Design is Disassociated Processing. Additionally CT.DP-P6 is not disassociated processing but a key tenant of Privacy by Design	Change the Category of Disassociated Processing to Privacy by Design. Make Disassociated Processing a subcategory of Privacy by Design to include P1-P3 & P5. P4 and P6 should be separate subcategories under Privacy by Design. In addition at P7 for use specification (only using collected for the reason specified at the time of collection). P8 completing a Privacy Risk Assessment and review during the develop of systems/platforms/organizational strategies.	Technical
11	Jennifer DiDonato/ Christine Eaton	28	Table 2	PR.DP-P9	Asser Management is key in on/off boarding to ensure there is no data leakage/loss. Asset Management should be included here in human resource practices.	Add asset management	Technical
12	Jennifer DiDonato/ Christine Eaton	28	Table 2	End	Respond should be added as a Function as addressed in comment 2		Technical
13	Jennifer DiDonato/ Christine Eaton	28	Table 2	End	Reassess should be added as a Function as described in comment 3.	For the Reassess Function it would have the following Categories: Annual Assessment of Privacy Program; Review of Changes to Regulatory Landscape to include: Regulations, Cases, Fines, etc. ; Review Changes to Organizational Requirements: Location of Operations, risk appetite, forays into new technology, change in territorial scope, etc.	Technical

14	Jennifer DiDonato/ Christine Eaton	36	804	Appendix D	The Privacy Risk Assessment is too high level and not actionable. Organizations and individuals will come to this framework to help them develop their privacy stance. Throughout the framework the privacy risk assessment is referenced, but when the Appendix is consulted, it is very high-level. Unless an organization already had Privacy Risk Assessments in place, there is no instruction here on how to conduct one.	The Privacy Risk Assessment Section should contain a process for completing a privacy risk assessment to include suggested fields, steps, stakeholders, etc. An instructive template would be great. Also referencing other current Privacy assessments, may be helpful to identify these, PIA, DPIA, etc. You could reference those as industry standards to be consulted. Not required, but helpful to review.	Technical
15	Jennifer DiDonato/ Christine Eaton	Entire Document	Entire Document	Entire Document	I find that the framework is not actionable. The language is too high level. There is language on picking and choosing what you want for your privacy program. I understand what you're trying to achieve and a framework is not necessarily applicable to all organizations, but instead of a picking and choosing, an organization should go through the cores and conduct an analysis on whether or not to apply the item and a reasoning behind it, not a mere pick and choose.	I would add some more instructive almost step by step language. Like address each function, category and subcategory. If it does not apply note it and the reason why it does not apply. Document this for future review and future iterations. You can start by mentioning that the steps are purely instructive and not required, but then actually give organizations actionable steps to take if they want to comply with this framework.	Technical