From: Daniel Omiliak <domiliak@wcapra.com>
Sent: Thursday, October 24, 2019 7:19 PM
To: privacyframework <privacyframework@nist.gov>
Subject: NIST Privacy Framework: W. Capra Preliminary Draft Comments

Thank you for the opportunity to provide comment on the preliminary draft of the NIST Privacy Framework. We are excited about a common framework that may be used across various organizations to improve their privacy posture.

Attached are our comments.

Best Regards,

Danny Omiliak

Consultant

425-749-6043

221 N LaSalle St #1325

Chicago, IL 60601

www.wcapra.com

Comment #	Organization Name	Submitted By (Name/Email)	Page #	Line #	Section	Comment (Include rationale for comment)	Suggested Change	Type of Comment (General/Editorial/Technical)
1	W. Capra Consulting Group	Danny Omiliak domiliak@wcapra.com	4	130	1	The definition of privacy and PI data may be different across organizations, laws and standards bodies	"but also the means for achieving and defining it can vary"	General
2	W. Capra Consulting Group	Danny Omiliak domiliak@wcapra.com	4	140	1	Partnerships should be considered as part of a privacy design	Include "Strategic partnerships" in the list	General
3	W. Capra Consulting Group	Danny Omiliak domiliak@wcapra.com	7	195	1.1	The sensitivy of data should be considered a key lens for selecting an implementation tier. Risk is lower if the sensitive data that is collected or processed is low.	Include "Sensitivity of data" in the list	General
4	W. Capra Consulting Group	Danny Omiliak domiliak@wcapra.com	7	224	1.2.1	These problems are all relevant, but there's also the question of ownership of PI and the customer's awareness of what data is being collected about them.	"Problems can arise as unintended consequences from data processing that organizations conduct to meet their mission or business objectives especially when data subjects are unaware of their data being processed"	General

5	W. Capra Consulting Group	Danny Omiliak domiliak@wcapra.com	9	265	1.2.2	There is a conflict of interest for companies to evaluate the problems for individuals which will inevitably lead to a unrealistically low evaluations of risk	There should be a framework for companies to evaluate the potential risk of problems for individuals	General
6	W. Capra Consulting Group	Danny Omiliak domiliak@wcapra.com	9	276	1.2.2	There's also a component of revisiting the business/commercial purpose for which each data element is collected; perhaps not all data that is collected today should be collected tomorrow.	Additional sentence: "These assessments should include the evaluation of data collected today, the purpose of that data, and if it should continue to be collected considering the risks."	General
7	W. Capra Consulting Group	Danny Omiliak domiliak@wcapra.com	12	361	2.1	As part of Communicate, it is more than just an understanding but engaging and promoting an ongoing dialogue	"...enable organizations and individuals to have a reliable understanding, engage and promote a dialogue about how data are processed…"	General
8	W. Capra Consulting Group	Danny Omiliak domiliak@wcapra.com	13	396	2.2	The visual is a helpful tool for explaining this concept and should be moved farther up in the document when these ideas are first introduced	This visual should be moved to section 1.1	Editorial

9	W. Capra Consulting Group	Danny Omiliak domiliak@wcapra.com	13	405	2.3	Is this stating that Tier 2 is the minimum standard? Or is it saying that all companies should always strive to increase their Tier?	Call out more explicitly if a minimum standard is proposed	Editorial
10	W. Capra Consulting Group	Danny Omiliak domiliak@wcapra.com	15	469	3.2	Individual facing or third party facing employees who can be equipped to handle external questions regarding privacy should be included because consumer education is equally important	Include "employees in roles that interact with individuals should be equippped to handle questions regarding privacy"	General
11	W. Capra Consulting Group	Danny Omiliak domiliak@wcapra.com	16	506	3.3	Action plan should also include ongoing maintenance of directives already achieved so that they do not become gaps	"reflecting mission drivers, costs and benefits, risks, and a strategy for ongoing maintenance"	General
12	W. Capra Consulting Group	Danny Omiliak domiliak@wcapra.com	20	592	3.5	This is missing the execution of those requirements	"will be verified, validated, and fulfilled"	General

13	W. Capra Consulting Group	Danny Omiliak domiliak@wcapra.com	21		Table 2	There are subcategories that are missing from the "Inventory and Mapping" subcategories that would make this section more comprehensive	1. To whom data elements are shared with 2. The retention period of data elements 3. The business purpose or business criticality of data elements 4. The categorization of data elements into groups (e.g. Identifiers, Financial Information, Biometric Information).	Technical
14	W. Capra Consulting Group	Danny Omiliak domiliak@wcapra.com	21		Table 2	There are subcategories that are missing from the "Business Environment" subcategories that would make this section more comprehensive	1. Laws and regulations that apply to the organization	Technical
15	W. Capra Consulting Group	Danny Omiliak domiliak@wcapra.com	23		Table 2	There are subcategories that are missing from the "Awareness and Training" subcategories that would make this section more comprehensive	1. Employees that interact directly with individuals (e.g. call center agents, store associates) understand their roles and responsibilities as well as individuals' rights	Technical

16	W. Capra Consulting Group	Danny Omiliak domiliak@wcapra.com	24		Table 2	There are subcategories that are missing from the "Monitoring and Review" subcategories that would make this section more comprehensive	Policies, processes, and procedures for assessing new strategic partners, services providers, business processes or organizational changes are established and in place.	Technical
17	W. Capra Consulting Group	Danny Omiliak domiliak@wcapra.com	26		Table 2	Update the Data Security Definition to include individuals that the data belongs to, they are just as important to consider when it comes to privacy and authentication.	"is limited to authorized individuals, and the individuals the data is concerning, processes,…"	Technical
18	W. Capra Consulting Group	Danny Omiliak domiliak@wcapra.com	26		Table 2	There are subcategories that are missing from the "Identity Management, Authentication, and Access Control" subcategories that would make this section more comprehensive	Individuals are verified using reasonable authentication methods to access, correct, delete or perform another action on data about themselves	Technical