From: Shea Wynn (shwynn) <shwynn@cisco.com>
Sent: Thursday, October 24, 2019 4:22 PM
To: privacyframework <privacyframework@nist.gov>
Cc: Harvey Jang (hajang) <hajang@cisco.com>
Subject: NIST Privacy Framework: Preliminary Draft Comments

NIST Privacy Framework Team,

Thank you for the opportunity to submit comments on the preliminary draft of the NIST Privacy Framework. Please find attached our comments.

Best regards,

Shea

Shea Wynn

Americas Privacy Officer & Counsel

Cisco Systems, Inc.

Email: shwynn@cisco.com

Phone: +1 737 704 5050

Com-ment #	Organization Name	Submitted By (Name/Email)	Page #	Line #	Section	Comment (Include rationale for comment)	Suggested Change* * Suggested in-line edits reflected in red.	Type of Comment (General/Editorial/Technical)
1	Cisco Systems, Inc.	Shea Wynn/ shwynn@cisco.com	3	97-98	Executive Summary	Consider rephrasing the analogy regarding a house. A house in general needs to be well engineered and the foundation would need to match the room layout.	N/A	Editorial
2	Cisco Systems, Inc.	Shea Wynn/ shwynn@cisco.com	4	124-127	1	"Failure to manage privacy risks can have direct adverse consequences for people at both the individual and societal level, with follow-on effects on organizations' reputation, bottom line, and future prospects for growth." This is true for any risk. This does not add any specifics on why privacy risks should be managed over and above other categories of risks.	N/A	General/Editorial
3	Cisco Systems, Inc.	Shea Wynn/ shwynn@cisco.com	4	140-141	1	This should note that this is related to systems, products, and services that use personal data.	Taking privacy into account as they design and deploy systems, products, and services that use personal data and affect individuals.	Editorial
4	Cisco Systems, Inc.	Shea Wynn/ shwynn@cisco.com	4	142-143	1	Unintended impacts should also be mitigated.	Integrating privacy practices into their business processes that result in effective solutions to mitigate any unintended, adverse impacts;	Editorial
5	Cisco Systems, Inc.	Shea Wynn/ shwynn@cisco.com	4	144	1	Consider emphasizing transparency here.	Communicating and being transparent about these practices.	Editorial
6	Cisco Systems, Inc.	Shea Wynn/ shwynn@cisco.com	4	147	1	Consider including engineering and operations in the examples of the parts of an organzation's workforce that may be responsible.	Different parts of an organization's workforce, including executives, legal, engineering, operations, and information technology (IT) may take responsibility for different outcomes and activities.	General/Editorial
7	Cisco Systems, Inc.	Shea Wynn/ shwynn@cisco.com	5	183	1.1	Consider adding a short definition for Functions, Categories, and Subcategories.	N/A	General/Editorial
8	Cisco Systems, Inc.	Shea Wynn/ shwynn@cisco.com	6	208 (Figure 2)	1.2.1	Privacy risks should call out unintended consequences of data processing as it pertains to a specific person. It would be better to say associated with unintended consequences of processing an individual's data as opposed to imply data process. Unintended conquences of data processing can also occur to things (overload of the grid given sensor input), animals (tracking for sustainability gives data to hunters) and groups of people (human rights)	Privacy Risks associated with unintended consequences of processing an individual's data	Editorial
9	Cisco Systems, Inc.	Shea Wynn/ shwynn@cisco.com	7	235	1.2.1	It is not just an employee's privileges, it is also using data for a purpose beyond that for which the data was collected/captured/created that must be managed/protected. This purpose is often more tightly defined than a role of the processor.	N/A	General/Editorial

10	Cisco Systems, Inc.	Shea Wynn/ shwynn@cisco.com	7	257	1.2.2	Consider how privacy by design can fit into how privacy risks can be managed by an organization, ideally to avoid building systems, products, and services that create risks at the beginning stages.	N/A	General
11	Cisco Systems, Inc.	Shea Wynn/ shwynn@cisco.com	8	260-262	1.2.2	Organizations can also use insurance to share or transfer risk to other organizations.	Transferring or sharing the risk (e.g., insurance and 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);	Editorial
12	Cisco Systems, Inc.	Shea Wynn/ shwynn@cisco.com	8	278	1.2.3	These assessments are also a valuable tool for privacy professionals to use in communicating these risks, as well as potential business impact because of these risks, to internal stakeholders and senior business leaders.	N/A	General
13	Cisco Systems, Inc.	Shea Wynn/ shwynn@cisco.com	8	279-281	1.2.3	Consider revising to allow for the fact that an organization may accept certain problems for individuals after a full review of the situation.	Identifying if data processing could create unintended or unreasonable problems for individuals, even when an organization may be fully compliance with applicable laws or regulations, can help with ethical decision-making in system, product, and service design and deployment.	General/Editorial
14	Cisco Systems, Inc.	Shea Wynn/ shwynn@cisco.com	10	359-360	2.1	"Examples of Categories include: 'Data Management Policies, Processes, and Procedures' and 'Data Management.'" These sounds very similar. Consider replacing one of the examples with something else, such as something that discusses Purpose Management, 3rd Party Monitoring, or Data Subject Rights Management Policies.	N/A	Editorial
15	Cisco Systems, Inc.	Shea Wynn/ shwynn@cisco.com	10	364-365	2.1	Communication should include to individuals within an organization and also to individuals whose data is processed by that organization.	The Communicate-P Function recognizes that both organizations and individuals need to know how data are processed in order to manage privacy risk effectively. This includes communicating to organizations and individuals that participate in data processing activities and organizations, as well as organizations and individuals whose data are being processed.	Editorial
16	Cisco Systems, Inc.	Shea Wynn/ shwynn@cisco.com	11	381-384	2.2	It is unclear what an individuals' privacy needs include. However, it might make more sense for an organization to consider individuals' expectations of how their data is processed.	An organization determines these needs by considering organizational or industry sector goals, legal/regulatory requirements and industry best practices, the organization's risk management priorities, and the expectations of individuals who are part of—or directly or indirectly served or affected by—an organization's systems, products, or services.	Editorial

17	Cisco Systems, Inc.	Shea Wynn/ shwynn@cisco.com	11	385	2.2	Profiles are use to describe either the current or future state.	Profiles describe either the current state or the desired target state of specific privacy activities.	Editorial
18	Cisco Systems, Inc.	Shea Wynn/ shwynn@cisco.com	11	391-393	2.2	Profiles can also be used to assist in prioritizing activities to manage risks.	Profiles also can aid in communicating risk within and between organizations by helping organizations understand and compare the current or desired state of privacy outcomes and prioritize additional activities to manage an organization's privacy risk.	Editorial
19	Cisco Systems, Inc.	Shea Wynn/ shwynn@cisco.com	12	420-423	3	The Framework is a valuable tool to measure and balance privacy risks.	In either case, it is designed to complement existing business and system development operations, to provide a means of expressing privacy requirements to business partners and customers, to allow an organization to measure and balance privacy risks, and to support the identification of gaps in an organization's privacy practices.	Editorial
20	Cisco Systems, Inc.	Shea Wynn/ shwynn@cisco.com	12	433	3	The examples included in this section are not necessarily different ways the Framework can be used. They are more complimentary. If the Privacy Framework is used by an organization, ideally all of these examples can be undertaken at the same time when an organization creates their Current and Target Profiles.	The following subsections present a variety of ways in which organizations can use the Privacy Framework.	General
21	Cisco Systems, Inc.	Shea Wynn/ shwynn@cisco.com	14	505-507	3.3	The mission drivers, costs and benefits, and risks should be prioritized with the action plan.	Next, it creates an action plan to address gaps—prioritized to reflect mission drivers, costs and benefits, and risks—to achieve the outcomes in the Target Profile.	Editorial
22	Cisco Systems, Inc.	Shea Wynn/ shwynn@cisco.com	16	585	3.5	"Communication is especially important among entities in the data processing ecosystem." This sentence seems out of place. How does this point relate to the remainder of this paragraph or the preceding bullets?	N/A	General/Editorial
23	Cisco Systems, Inc.	Shea Wynn/ shwynn@cisco.com	18	637	Appendix A	The draft states that the Core is not exhaustive. This point is especially important for organizations that might have unique issues due to the nature of the personal data they are processing or because of their role in the data processing ecosystem. Consider providing a bit more context or examples of additional considerations that organziations might need to consider that is not captures in the current draft of the Core. Also, this point can be used to allow organizations to better adapt to emerging technologies that might create new concerns or privacy compliance needs that should be included in the Profiles going forward. Consider discussing how the current Core can be tailored to address new issues that are created by these emerging technologies.	N/A	General

24	Cisco Systems, Inc.	Shea Wynn/ shwynn@cisco.com	18	641	Appendix A	The term "workforce" as the introduction to this bullet seems like it could be confusing. Consider replacing with the suggested change.	Within an Organization	Editorial
25	Cisco Systems, Inc.	Shea Wynn/ shwynn@cisco.com	18	646	Appendix A	To match the suggested change above, consider revising the second bullet introduction.	Within the Data Processing Ecosystem	Editorial
26	Cisco Systems, Inc.	Shea Wynn/ shwynn@cisco.com	19	653	Appendix A	The term "scalability" as the introduction to this bullet seems like it could be confusing.	Flexibility	Editorial
27	Cisco Systems, Inc.	Shea Wynn/ shwynn@cisco.com	19	664-670	Appendix A	Consider revising the remainder of this paragraph. It is unclear what you are proposing organizations do if they are not utilizing the Cybersecurity Framework in conjuction with the Privacy Framework. Is the suggestion that organizations should use the Detect, Respond, and Recover Functions as part of the Privacy Framework if they are not already addressing those Functions as part of the Cybersecurity Framework? If so, the Categories and Subcategories of those Functions should be included in the Privacy Framework Core detailed in Table 2.	N/A	General/Editorial
28	Cisco Systems, Inc.	Shea Wynn/ shwynn@cisco.com	21	684	Category - Inventory and Mapping	Which Subcategory would include inventorying third parties to whom data is disclosed and for what purposes? Consider making it clearer if it is intended to be included in one of the existing Subcategories or adding an additional one.	N/A	General
29	Cisco Systems, Inc.	Shea Wynn/ shwynn@cisco.com	21	684	ID-IM-P1	Consider defining what is meant by “inventoried” in the glossary. At a high level, what information should organizations be collecting and recording as part of their inventory?	N/A	General
30	Cisco Systems, Inc.	Shea Wynn/ shwynn@cisco.com	21	684	ID.IM-P5	Is the agreed upon purpose of the data inventoried here given the legal basis under which it was collected/captured/created? Or just the data actions (what the action results in)? Consider clarifying. Is the data inventoried as personal information or in a collection that makes it personal information?	N/A	General
31	Cisco Systems, Inc.	Shea Wynn/ shwynn@cisco.com	21	684	ID.BE-P3	Consider whether it is useful to also identify systems/products/services that support business critical operations.	Systems/products/services that support organizational priorities and/or that support business critical operations are identified and key requirements communicated.	Editorial
32	Cisco Systems, Inc.	Shea Wynn/ shwynn@cisco.com	22	684	Risk Assessment	Aren’t the gaps identified by comparing Current and Target Profiles also a kind of privacy risk assessment? Consider clarifying that these risk assessments take into account these gaps when formulating the action plan described in lines 505-507 of the Framework.	N/A	General

33	Cisco Systems, Inc.	Shea Wynn/ shwynn@cisco.com	22	684	ID.DE-P1	What kind of processes is this Subcategory intending an organization create and how are they different than the subsequent subcategories? As an action item, this seems vague and unclear.	N/A	General
34	Cisco Systems, Inc.	Shea Wynn/ shwynn@cisco.com	23	684	GV.RM-P2	This Subcategory should also ensure that the risk tolerance is documented.	Organizational risk tolerance is determined, documented, and clearly expressed.	Editorial
35	Cisco Systems, Inc.	Shea Wynn/ shwynn@cisco.com	23	684	GV.RM-P3	This does not seem like it should be a Subcategory. Consider moving this sentence to the end of the paragraph in the related Category.	N/A	General/Editorial
36	Cisco Systems, Inc.	Shea Wynn/ shwynn@cisco.com	23	684	GV.AT-P1	Does this include user (Data Subjects Rights) training?	The workforce is informed and trained on its roles and responsibilities, including with regards to individual users' requests.	General/Editorial
37	Cisco Systems, Inc.	Shea Wynn/ shwynn@cisco.com	24	684	CT.PO-P2	Does this cover the organzation or the data subject or both? Where is keeping the data updated covered (i.e., alteration)?	N/A	General
38	Cisco Systems, Inc.	Shea Wynn/ shwynn@cisco.com	24	684	CT.PO-P3	Consider also calling out individuals' choices as well.	Policies, processes, and procedures for enabling individuals' data processing preferences, choices, and requests are established and in place.	Editorial
39	Cisco Systems, Inc.	Shea Wynn/ shwynn@cisco.com	25	684	CT.DM-P5	It states data are destroyed according to policy, but consider clarifying that this requires the policy covers all necessary privacy requirements (e.g., minimization of data, data subjects rights).	N/A	General
40	Cisco Systems, Inc.	Shea Wynn/ shwynn@cisco.com	25	684	CT.DP-P1	There may be situations where it would not make sense to process data in an unobservable or unlinkable manner. Consider adding "when possible."	Data are processed in an unobservable or unlinkable manner (e.g., data actions take place on local devices, privacy-preserving cryptography) when possible.	General/Editorial
41	Cisco Systems, Inc.	Shea Wynn/ shwynn@cisco.com	25	684	CT.DP-P2	There may be situations where it would not make sense to limit the identificaiton of individuals. Consider adding "when possible."	Data are processed to limit the identification of individuals (e.g., differential privacy techniques, tokenization) when possible.	General/Editorial
42	Cisco Systems, Inc.	Shea Wynn/ shwynn@cisco.com	25	684	CT.DP-P5	There may be situations where it would not make sense to substitute attribute values with attribute references. Consider adding "when possible."	Attribute references are substituted for attribute values when possible.	General/Editorial
43	Cisco Systems, Inc.	Shea Wynn/ shwynn@cisco.com	25	684	CM.PP-P1	It should be clear that these policies, processes, and procedures should be disclosed as applicable.	Transparency policies, processes, and procedures for communicating data processing purposes, practices, and associated privacy risks are established, in place, and disclosed as applicable.	Editorial
44	Cisco Systems, Inc.	Shea Wynn/ shwynn@cisco.com	26	684	CM.AW-P7	There may be situations where notice is not apporpriate or necessary (e.g., due to the limited data involved, the nature of the event, or in response to requests from authorities). Consider adding "when necessary" to make this clear.	Impacted individuals and organizations are notified about a privacy breach or event when necessary.	General/Editorial

45	Cisco Systems, Inc.	Shea Wynn/ shwynn@cisco.com	26	684	PR.AC-P5	The Subcategory offers network segregation and network segmentation as examples. Should this be data storage/data processing segregation and segmentation?	N/A	General
46	Cisco Systems, Inc.	Shea Wynn/ shwynn@cisco.com	33	722-731	Appendix D	This section makes sense but consider whether the Privacy Framework should advise that there be a single individual or team with the ultimate responsibility and authority for overseeing an organization's privacy compliance. While certain tasks may be the responsibility of various teams and the input of different stakeholders can be useful, having a team or individual responsible for privacy within an organization would ensure there is a primary point of contact and decisionmaker, as well as someone that will be required to consider all aspects of the privacy program.	N/A	Editorial
47	Cisco Systems, Inc.	Shea Wynn/ shwynn@cisco.com	33-34	740-749	Appendix D	See Comment 30 above.	N/A	Editorial
48	Cisco Systems, Inc.	Shea Wynn/ shwynn@cisco.com	34	760-763	Appendix D	Consider replacing the term "artifacts" with another word, such as "plans."	System/product/service design plans (ID.BE-P3) Design plans may take many forms such as system design architectures or data flow diagrams. These plans help an organization build systems, products, and services that meet an organization's mission/business priorities and objectives. ... A data map can be overlaid on existing system/product/service design plans for convenience and ease of communication between organizational components.	Editorial
49	Cisco Systems, Inc.	Shea Wynn/ shwynn@cisco.com	34	774	Appendix D	See Comment 32 above.	As discussed below, a data map is an important component of a privacy risk assessment	Editorial
50	Cisco Systems, Inc.	Shea Wynn/ shwynn@cisco.com	35	794	Appendix D	Is this section intended to cover privacy requirements for a specific system, product, or service or requirements that every system, product, or service should meet? The first sentence seems to indicate the former, but the last two sentences seem to indicate the latter.	N/A	General/Editorial
51	Cisco Systems, Inc.	Shea Wynn/ shwynn@cisco.com	36	832	Appendix D	"As noted in Section 1.2, the experience of individuals is a type of externality for organizations." This sentence is confusing. What is it trying to say and what part of section 1.2 is it referencing?	N/A	General/Editorial