Comments on the Public Draft of the NIST Privacy Workforce Taxonomy

January 16th, 2025

by
Anza Abbas (Enterprivacy Consulting Group)
Andrew Berry (Enterprivacy Consulting Group)
R. Jason Cronk (Enterprivacy Consulting Group & Institute of Operational Privacy Design)
Nandita Narla (Institute of Operational Privacy Design)
Vandana Padmanabhan (Independent)

1. Are these TKS Statements drafted at a helpful level of detail?

The statements are generally at a helpful level of detail although some are unnecessarily wordy. In fact, most of our suggested rewrites are to simplify and clarify the statements. Statements should be terse but complete. Several statements use superfluous clauses, are overly wordy or use terminology that does not match the Privacy Framework. Many are just parroting the words of the subcategory, which seems to demonstrate a lack of understanding of their meaning by the drafters. To be fair, some of the subcategories are convoluted. We have suggested editing or removing superfluous clauses or non-standard terms.

We also noticed that NIST removed many of the parentheticals. While this makes the statements clearer and easier to read, it could remove some context and clues for readers who may be unfamiliar with some of the concepts. Additional supportive or clarifying text for many of the statements would also be helpful.

2. Are any TKS Statements missing? Are any TKS Statements unnecessary or irrelevant?

In the provided spreadsheet, we have suggested adding, dropping or replacing statements to the subcategories.

Added statements are marked "**Add**" in green, in column E ("Recommendation"), in the Mapping tab. If the recommendation is for an existing statement used elsewhere, the statement ID is included in Column B. Some of the additions come from Version 7 of the TKS Statements published in draft form to the PWWG but later dropped by NIST. This is usually mentioned in column F ("Comments") or indicated in Column B. Several subcategories lacked statements to sufficiently or completely meet the outcomes in the subcategory. Some statements were added because they fit into the subcategory (but were not mapped) or in lieu of other statements.

Statements recommended to be dropped are marked “**Drop**” in red in column E (“Recommendation”). An explanation of why we suggest dropping the statement is included in column F (“Comments”). Many statements went beyond the scope of the subcategory. Some seemed completely unrelated. Some statements were convoluted and unsalvageable.

Statements recommended to be replaced are marked “**Replace**” in blue in Column E (“Recommendation”). In the comments, we note the recommended replacement statement which usually appears directly below following the above convention for adding a statement.

The subcategories contain lots of meta-tasks (i.e. tasks that don't achieve the outcome but are indirectly supportive of the outcome, more *likely* occurring). For instance, if the outcome is “the tire is changed,” a task to support that outcome is "take the old tire off." A meta-task would be "have a procedure for removing an old tire.” Yes, that would be helpful but it goes down a rabbit hole. Similarly, many of NIST’s policies, procedures, mechanisms, tools, etc. are helpful at achieving the outcome but don't directly result in the outcome happening. One can easily have a procedure to change a tire and not actually get the tire changed. The steps in the procedure would be the relevant tasks to achieve the outcome, not the creation of the procedure. There are specific subcategories that have those supporting activities (i.e. most of the PO categories). We sometimes left such supporting statements unchanged but other times, recommended they be dropped.

Where we recommended dropping statements and those statements no longer relate to any subcategory, we have recommended dropping the statement entirely in the relevant statements tabs. Sometimes, we have provided alternative phrasing to deletion, in case NIST decides to keep the statements despite the recommendation.

3. Is the "Notes" section that is included in certain Subcategory mappings (e.g., ID.BE-P2) useful? Are there other Subcategories that would benefit from notes? If so, what Subcategories? What information would be useful to include in these additional notes?

We hold no strong opinion on the notes. In general, we find that the terseness of the subcategories and the statements warrant additional guidance.

4. Are the TKS Statements mapped to the appropriate Subcategories?

As stated in our answer to question #2, we provided instances of where we recommend adding or replacing statements with more appropriate ones. We noticed there are a number of broadly useful knowledge and skill statements that appear in a limited one or two subcategories for no understandable reason. See K304 (“Knowledge of the organization's technical environment.”), which could be helpful in many areas but only appears in one subcategory. Another example, S258 (“Skill in privacy engineering”) could be useful throughout the CT.DM and CT.PD categories but is only found in CT.DM-P5 and CM.AW-P3. We recommended dropping it from the former subcategory rather than recommending it across the categories.

This begs the question of why NIST decided against the approach of designating certain knowledge and skills as broadly applicable. For instance, K257 ("Knowledge of the organization's data processing") applies to 30 subcategories out of 70 total. This results in a lot of duplicate bulk in the taxonomy.

We did not update the mapping in Column D in the Mapping tab or Column C in the statement tabs, leaving that to NIST once our recommendations have been adjudicated.

5. Do the organization-defined parameters bracketed within TKS Statements provide helpful flexibility for organizations seeking to tailor TKS Statements to their needs?

Task statements should not contain the statement about organization-defined frequency. This could apply to **all** the tasks. The organization is going to determine how often the tasks need to be done: once, annually, quarterly or even daily. We've recommended NIST remove all references to organization-defined frequency.

Organization-defined stakeholders are not necessary in many tasks. Clearly, the person performing nearly any tasks for the organization could consult with others. In fact, many stakeholders are going to be tasked with performing the tasks. For instance, T184 ("Draft privacy breach or event communications in consultation with [*organization-defined stakeholders*].") Anyone consulted on a draft communication would be one of the people performing the drafting task. There isn't one person drafting and consulting with others. All of the people involved are "drafting." We generally recommended removing organization-defined stakeholders unless the subcategory called for some separation of duty.

6. Should Task Statements focused on creating documentation (i.e., T155 - T182) be included? If so, are any changes to these Task Statements necessary (i.e., additions, subtractions, revisions)?

We hold no strong opinion holistically on the documentation tasks. We did recommend dropping some.

Recommendations for Updating Statements

We have many recommendations for updating statements. Most of these recommendations are for the purpose of simplifying, clarifying or making the statements more relevant to the subcategory. Where we suggested updating, we have marked in the Mapping tab with "**Update"**, in column E ("Recommendation") and put a comment to see the recommended update in the relevant statement tab. In the relevant statement tab, you will find the recommended rewriting of the statement in column F ("Suggested Statement") and our justification, explanation or reasoning in column E ("Comments").

In general, the skills statements "in applying" should be more explicit as to how you are "applying" something. For instance, for S023 (“Skill in applying data minimization techniques to achieve data utility and de-identification requirements.”), we have recommended changing to “Skill in minimizing data” for the purposes of reducing the link, being more direct in phrasing and removing the objective. You will also find that we have provided an alternative statement, should NIST adjudicate our recommendation too narrow. The alternative, for this statement, is “Skill in minimizing data while maintaining data utility.”

In general, we found too much use of "privacy" as an adjective modifier. Our opinion is that it just adds words without conveying important meaning. In some instance, it was incorrectly applied restricting the scope of the statement (such as saying privacy risk management instead of the broader corporate area of risk management). In many cases, we have recommended updating the statements to reflect the unnecessary application of the term “privacy.”

We have recommended removing from statements any specificity of "a" or "the" system/product/service. For example, for directing a command to someone to perform a task, say: “review **the** system;” but for such tasks being performed by the organization or someone, the specificity should be dropped, to simply say: “review systems.”

Some additional commentary appears in a few red highlighted boxes in the Mapping tab.

We hope NIST and the broader privacy community finds these comments and suggested edits helpful and useful.