NIST PRIVACY WORKFORCE PUBLIC WORKING GROUP (PWWG)

Co-Chair: Dylan Gilbert, NIST Privacy Policy Advisor

MONTHLY MEETING MINUTES
Wednesday, August 9, 2023
1:00 P.M. ET – 2:00 P.M. ET

I. INTRODUCTION

The 26th meeting of the National Institute of Standards and Technology (NIST) Privacy Workforce Public Working Group (PWWG) convened on Wednesday, August 9th from 1:00 P.M. - 2:00 P.M. ET virtually via Microsoft Teams. There were 44 attendees.

The PWWG provides a forum for participants from the public, including private industry, the public sector, academia, and civil society, to create the content of the NIST Privacy Workforce Taxonomy. The PWWG is tasked with creating Task, Knowledge, and Skill (TKS) Statements aligned with the NIST Privacy Framework and the National Initiative for Cybersecurity Education (NICE) Workforce Framework for Cybersecurity.

PWWG Co-Chair, Dylan Gilbert, welcomed attendees and Project Teams Co-Leads and thanked them for their participation. Dylan noted that Co-Chair Doug Forman was also present on the call.

II. PWWG UPDATE

A. TKS CONFORMANCE COMMITTEE - TKS COMPILATION INVENTORY AND MAPPING DOCUMENTS

During the August PWWG meeting Dylan announced that the TKS Compilation Inventory and TKS Compilation Mapping documents had been updated to reflect the work done to date by the first five Project Teams. These documents contain a running inventory of approximately 750 TKS Statements that were completed over the past two years. At the September PWWG Meeting Dylan plans to announce another update to these Inventory and Mapping documents which will incorporate the work done to standardize the TKS Statements.

B. TKS STANDARDIZATION

Dylan provided an update on the work of the NIST TKS Conformance Committee. The NIST team decided that the conformance, or standardization, work would be undertaken by the NIST Privacy Team. There are three goals for the conformance process: to provide line edits for syntax and Authoring Guide conformity; to leverage the NICE “Style Guide” for further standardization; and to generate PWWG-specific rules.

Dylan noted that the heavier lift is what he loosely referred to as a style guide. The team at the National Initiative for Cybersecurity Education (NICE) have been updating the TKS Statements aligned with Revision 1 of the NICE Workforce Framework. As part of their process, they created some style rules to ensure that their TKS Statements are standardized. It is a priority for the NIST Privacy Engineering Program (PEP) to align its material as much as possible with the NICE Framework material. There will be some key differences that are specific to the Privacy Framework. To the extent that there are differences or rules specific to the PWWG, the Conformance Committee has been working to generate those rules as well.

C. EXAMPLES OF TKS STANDARDIZATION

1. How should TKS Statements generally refer to stakeholders?

Dylan shared an example of a rule that was identified by the Conformance Committee. He noted that anyone who has participated in a project team will recognize that the term, "stakeholders”, comes up frequently. They often need to be collaborated with or consulted or identified when it comes to achieving outcomes in the

Privacy Framework. There were many varied ways of referencing Stakeholders in the TKS Statements. The Team decided upon a standardized format, organization-defined parameters, which will be familiar to those who use Special Publication (SP) 800-53 (Rev 5). SP 800-53 is a consolidation of privacy and cybersecurity controls which has been mapped to the Privacy Framework. The PWWG taxonomy will use the bracketed term, [*organization-defined stakeholders*], to note that it's up to the organization to define the stakeholders in a given context. This provides maximum flexibility for organizations.

The following PWWG Task Statement conforms to this rule:

- Finalize privacy policies with approval from [*organization-defined stakeholders*].

Dylan noted that there will always be exceptions, and one exception in the Privacy Framework is where it specifically calls out third-party stakeholders, such as:

- Identify third-party stakeholder roles and responsibilities to support privacy policies/processes/procedures.

In this case, it's necessary to specify that there are third-party stakeholder roles without specifying who the third-party stakeholders are.

Question from chat: Would this include defining 'privacy engineer' roles & responsibilities? There are a lot of engineers and a lot of initiatives trying to define the terms 'Privacy Engineering' or 'Privacy Engineer'. I'm interested to know whether this might also include doing that, or defining of roles and responsibilities?

Dylan replied that if there was a third-party stakeholder that had a role or responsibility to support the organization's privacy policies or procedures then a privacy engineer could fall under that third-party umbrella. There is no definition for Privacy Engineer in the Privacy Framework.

Dylan noted that, once the TKS Statements are complete, he hopes to have a larger conversation about a second phase of the PWWG. It may be to consider work roles, or perhaps competencies, aligned with the NICE Framework. For example, the PWWG could consider what Tasks would be involved in a Privacy Engineering role, or a Privacy Architect role.

2. **How can we avoid multiple TKS Statements for common phrases in the PF (e.g., policies, processes, and procedures)?**

Some of the teams have been grappling with certain phrases that show up a lot in the Privacy Framework, often with commas, such as, 'policies, processes, and procedures' and 'mission, objectives, and activities.' In order to adhere to the Authoring Guide, multiple Statements are required for these, one Task for policies, one for processes, etc. The Conformance Committee decided that these commonly occurring phrases would be grouped together with slashes.

Examples of these combined Statements:

- Knowledge of how system/product/service inventories are organized.
- Knowledge of existing policies/processes/procedures.

3. **How can we streamline statements that contain assumed knowledge or activities?**

Dylan noted that the next type of Statement that the Conformance Team has identified as needing a rule is, for lack of a better term, assumed knowledge or activities.

As the team reviewed the totality of the Statements which contained knowledge or activities which they think should be assumed, they wanted to pull those things out of the Statements and define and address the assumed knowledge and activities within the taxonomy and put it either in the front matter or in an appendix. As an example, a Statement relating to establishing organizational roles where necessary and feasible to support third parties, stakeholder privacy, and risk management responsibilities. Generally, most of this can be pulled out and

it will say, unless otherwise indicated, assume that this is referring to the organization. Also assume that a Task is necessary to do that.

An example of this would be:

- **Example Old "Assumed Knowledge" Statement:** Establish organizational roles, where necessary and feasible, to support third-party stakeholder privacy risk management responsibilities.
    - **Example Updated "Assumed Knowledge" Statement:** Establish a role(s) to support third-party stakeholder privacy risk management responsibilities.

There are going to be places where we will need to call out certain things, so we're being careful to make sure that we don't eliminate Statements where this information actually is applicable, as in the following example:

- **Example: Retained "Organization Specific" Statement:** Knowledge of the organization's contract management practices (e.g., storage, location, responsible entity).

In the next example of an assumed activity, 'document organizational privacy values', and 'maintain documentation of organizational primacy values', there was a lot of conversation around this early on. It is a bit of a controversial topic, this idea of whether there is a need to have specific Tasks around maintaining documentation. What the Conformance Committee decided was to view this as an assumed activity.

- **Example Old "Assumed Activity" Statements:**
  Document organizational privacy values.
  Maintain documentation of organizational privacy values.
    - **Example Updated "Assumed Activity" Statement:** Document organizational privacy values.

The Conformance Committee expects to complete its work in the next week, and Dylan will present the updated TKS Inventory and Mapping documents at the September meeting.

D. COMPLETION OF ID.RA-P2 TKS STATEMENTS

Dylan announced that he has been working with the NIST AI team to finalize the TKS Statements for Subcategory ID.RA-P2. He expects to be able to include ID.RA-P2 TKS Statements in the updated TKS Inventory and Mapping documents in time for the September PWWG meeting.

III. Project Team Updates

A. UPDATE OF PROJECT TEAM 6: RISK MANAGEMENT STRATEGY

GOVERN-P (GV-P): Develop and implement the organizational governance structure to enable an ongoing understanding of the organization's risk management priorities that are informed by privacy risk.

- **Risk Management Strategy (GV.RM-P)**: The organization's priorities, constraints, risk tolerances, and assumptions are established and used to support operational risk decisions.
    - **GV.RM-P1:** Risk management processes are established, managed, and agreed to by organizational stakeholders.
    - **GV.RM-P2**: Organizational risk tolerance is determined and clearly expressed.
    - **GV.RM-P3**: The organization's determination of risk tolerance is informed by its role(s) in the data processing ecosystem.

Dylan gave the update for PT6. There are 3 Subcategories around establishing risk management processes, making sure that the organization's risk tolerance is determined, and then using that risk tolerance to inform the organization's role in the data processing ecosystem. The goal for PT6 was to complete work for the first Subcategory on establishing, managing, and finalizing risk management processes. They are almost done with that Subcategory, and Dylan has suggested that they move on to Subcategory GV.RM-P2. The Co-Chairs will review the TKS Statements for GV.RM-P1 at their next meeting and provide feedback.

The ongoing challenge for PT6 has been walking the line between where privacy comes in and where it is not required. GV.RM-P1 does not say 'privacy' risk management processes are established. The Privacy Framework is an enterprise privacy risk management tool, so in order to do privacy risk management, there needs to be overall enterprise level risk management processes in place. The team generally has had conversations around what role privacy plays versus the overall risk management processes as they're putting together their TKS Statements.

B. UPDATE OF PROJECT TEAM 7: Awareness and training (GV.AT-P)

GOVERN-P (GV-P): Develop and implement the organizational governance structure to enable an ongoing understanding of the organization's risk management priorities that are informed by privacy risk.

- **Awareness and Training (GV.AT-P):** The organization's workforce and third parties engaged in data processing are provided privacy awareness education and are trained to perform their privacy-related duties and responsibilities consistent with related policies, processes, procedures, and agreements and organizational privacy values.
    - **GV.AT-P1**: The workforce is informed and trained on its roles and responsibilities.
    - **GV.AT-P2**: Senior executives understand their roles and responsibilities.
    - **GV.AT-P3**: Privacy personnel understand their roles and responsibilities.
    - **GV.AT-P4**: Third parties (e.g., service providers, customers, partners) understand their roles and responsibilities.

Project Team 7 Co-Lead, Jacqueline Crowley provided the team update for PT7. The team is currently working on TKS Statements for GV.AT-P1. The Co-Chairs have already provided feedback for some of the Task Statements. Jacqueline expects the team to complete Subcategory GV.AT-P1 at the next meeting and send the remaining TKS Statements for Co-Chairs.

Jacqueline encouraged members to review the TKS Statements offline and leave any comments in the PT7 Google Workbook.

C. UPDATE OF PROJECT TEAM 8: DATA PROCESSING MANAGEMENT (CT.DM-P)

CONTROL-P (CT-P): Develop and implement appropriate activities to enable organizations or individuals to manage data with sufficient granularity to manage privacy risks.

- **Data Processing Management (CT.DM-P**): Data are managed consistent with the organization's risk strategy to protect individuals' privacy, increase manageability, and enable the implementation of privacy principles (e.g., individual participation, data quality, data minimization).
    - **CT.DM-P1**: Data elements can be accessed for review.
    - **CT.DM-P2**: Data elements can be accessed for transmission or disclosure.
    - **CT.DM-P3**: Data elements can be accessed for alteration.
    - **CT.DM-P4**: Data elements can be accessed for deletion.
    - **CT.DM-P5**: Data are destroyed according to policy.
    - **CT.DM-P6**: Data are transmitted using standardized formats.
    - **CT.DM-P7**: Mechanisms for transmitting processing permissions and related data values with data elements are established and in place.
    - **CT.DM-P8**: Audit/log records are determined, documented, implemented, and reviewed in accordance with policy and incorporating the principle of data minimization.
    - **CT.DM-P9:** Technical measures implemented to manage data processing are tested and assessed.

- **CT.DM-P10**: Stakeholder privacy preferences are included in algorithmic design objectives and outputs are evaluated against these preferences.

Project Team 8 Co-Lead, Nikita Samarin, provided the update. The team is currently working on TKS Statements for CT.DM-P1. Nikita noted there are ten different Subcategories but the first five are very similar in that they affect data elements in different operations.

The Co-Leads have finalized the TKS Statements for P1 and will share with the team on the call next week. The team has been trying to balance the level of granularity with specificity. Nikita believes that is the biggest challenge facing PT8, to make sure that the statements are applicable to a variety of organizations, whether they are using off the shelf tools or if they're addressing technology in-house. Nikita noted that the team has had very productive and engaging discussions during PT8 meetings.

The Co-Leads are hoping to be able to easily complete drafting Statements for P2-P5 because of the similarities with CT-DM-P1. The Co-Leads will then continue drafting Statements for the remaining Subcategories, CT-DM-P6-P10.

Dylan noted that there has been some conversation about this on the PT8 Google listserv. The first four Subcategories in particularly are just variations on a theme. The Co-Chairs will be able to look at the Subcategories P1-P5 as a block.

Dylan reminded all Project Team members that the intent is for work to happen outside of team meetings. All members are encouraged to review and submit comments in the Google Workbooks between meetings so that the teams can discuss these ideas during the scheduled meetings.

IV. Q & A

V. NEXT STEPS & UPCOMING MEETINGS

A. NEXT STEPS

Join a project team! The mailing lists are now live. Sign up for any team or all of teams! The team Leads will soon send out a welcome note via the Google Group mailing list.

- PT6 (GV.RM-P): PrivacyWorkforcePT6+subscribe@list.nist.gov
- PT7 (GV.AT-P): PrivacyWorkforcePT7+subscribe@list.nist.gov
- PT8 (CT.DM-P): PrivacyWorkforcePT8+subscribe@list.nist.gov

B. UPCOMING MEETINGS

The upcoming meetings of the NIST PWWG and its Project Teams are noted below. For further information, including updated meeting schedules, meeting minutes, agendas, and slide deck please visit the PWWG web page.

Project Team 6 (PT6)

- Next Meeting: Thursday, August 10, 2023 | 1:00pm – 2:00pm ET

Project Team 7 (PT7)

- Third Meeting: Wednesday, August 16, 2023 | 1:00pm – 2:00pm ET

Project Team 8 (PT8)

- Third Meeting: Thursday, August 17, 2023 | 11:00am – 12:00pm ET

NIST Privacy Workforce Public Working Group

- Wednesday, September 13, 2023 | 1:00pm – 2:00pm ET

C. NEW BUSINESS OPEN TOPICS

New Business Open Discussion Topics Drop Box is available on the NIST Privacy Workforce Working Group webpage. If you are interested in presenting a business topic during a PWWG Monthly Meeting, please visit the webpage noted above.

D. TROUBLESHOOTING

If you have any technical issues with meeting invitations, mailing lists, and/or accessing the Google Drives, please email NIST PWWG Support at PWWG@nist.gov.

E. JOIN MAILING LIST

To join one of the Project Teams you must subscribe to its associated mailing list. All mailing lists are moderated. Please be reminded to adhere to the Mailing List Rules that can be found on the NIST Privacy Workforce Working Group website.

- PWWG: PrivacyWorkforceWG+subscribe@list.nist.gov
- PT6 (GV.RM-P): PrivacyWorkforcePT6+subscribe@list.nist.gov
- PT7 (GV.AT-P): PrivacyWorkforcePT7+subscribe@list.nist.gov
- PT8 (CT.DM-P): PrivacyWorkforcePT8+subscribe@list.nist.gov