NIST PRIVACY WORKFORCE PUBLIC WORKING GROUP (PWWG)

Co-Chair: Dylan Gilbert, Privacy Policy Advisor, National Institute of Standards and Technology

MEETING MINUTES
Wednesday, April 13, 2022
1:00 P.M. EDT – 2:00 P.M. EDT

I. INTRODUCTION

The 12th meeting of the National Institute of Standards and Technology (NIST) Privacy Workforce Public Working Group (PWWG) convened on Wednesday, April 13th, 2022 from 1:00 P.M. - 2:00 P.M. EDT virtually via Microsoft Teams.

Co-Chair, Dylan Gilbert, NIST Privacy Policy Advisor, welcomed the members and Project Teams Leads and thanked them for their participation. Dylan provided a brief overview of the meeting agenda which included: a review of NIST Privacy Framework and PWWG Task, Knowledge, and Skill (TKS) Mapping documents; PWWG Co-Chair Review of TKS Statements; Resources discussion; and Project Team updates.

II. PWWG UPDATES

Co-Chair: Dylan Gilbert provided a brief update of the general status of the PWWG Project Teams and activities.

A. NIST PRIVACY FRAMEWORK AND PWWG TKS MAPPING

Dylan discussed the PWWG TKS Statements mapping documents that include Project Team 2's Inventory and Mapping, ID.IM-P (*Data processing by systems, products, or services is understood and informs the management of privacy risk)* TKS statements that have received final approval from the PWWG Co-Chairs.

All PWWG members have access to these reference documents. The documents are saved as read-only PDFs in the PWWG Reference Documents[1] folder on the shared Google Drive. The TKS statements are mapped to the Privacy Framework Core[2], specifically to the Inventory and Mapping Category in the Identify-P Function, which was the assignment for Project Team 2 (PT2). The goal was to keep the mapping as simple as possible. There will be an opportunity at a later date to offer feedback on this material, and the group should think through what final form the TKS Statements should take for the users of the final product.

There will be slight variations in the way that these mappings were approached by the different Project Teams. At the end of this process, the PWWG will set up a conformance committee to resolve any inconsistencies.

Dylan then provided a brief overview of the PWWG TKS Statements – Inventory Reference Document[3] and the PWWG TKS Statements – Subcategories Reference Document[4].

[1] PWWG Reference Documents Folder
[2] NIST Privacy Framework Core (pdf)
[3] PWWG TKS Statements – Inventory Reference Document
[4] PWWG TKS Statements – Subcategories Reference Document

i. PWWG TKS Statements – Inventory Reference Document[3]

- Tasks, Knowledge and Skills are listed in alphabetical order.
- When listed in alphabetical order, dependencies are not together - e.g., 'identify' needs to happen before 'document' and these tasks are not shown in the correct order.
- Team members are encouraged to think about this and discuss with their team(s) whether they find this approach confusing.

The PWWG Co-Chairs would like to hear from working group members what they believe is the most helpful way to present this information for members' organizations and teams.

The use of parentheticals within a TKS Statement

- Some tasks include parentheticals where the team thought it would be useful to provide examples. E.g., Task T004: *Define categories of data processing environments (e.g., cloud, on premises, geographic locations, jurisdictions, etc.)*
- For efficiency, the use of the collective term, 'system, product, and service' is used, rather than repeat each task three times.

The referencing of Regulations/Laws within a TKS Statement.

- Brackets are used in some TKS statements – e.g., K001: *Knowledge of [organization selected regulation-defined] roles of system/product/service and component owners or operators*. This example is similar to what is used in NIST SP 800-53[5], in which the organization can select what the particular regulation defined role is.
- Other project teams may take another tack, if they feel they can't capture this in an agnostic way. This would be a first example for a conformance activity.
- There were questions from the members regarding terms used: the use of regulation versus law; the use of the term, 'select' with respect to an externally defined law. Members are encouraged to incorporate these edits and clarifications into the work of their Project Teams.

ii. PWWG TKS Statements – Subcategories Reference Document[4]

- TKS statements are listed as they are mapped to Subcategories.
- PT2 also mapped statements at the Category level. They found it helpful to get the level of granularity they wanted by level-setting in this way, rather than being duplicative.
- This is not required. Other teams may do that if they want.

Mapping at Category/Subcategory Level

Dylan noted that the working group needs to consider how to approach the mapping, whether at the Subcategory level only, or also at the Category level. The PWWG Co-Chairs don't want to mandate mapping only at the Subcategory level since Project Team 2 found it helpful to get their work done. There may potentially be some inconsistencies. The PWWG will need to conform this once all the work is done.

- There is a potential pitfall in itemizing the statements in alphabetical order. Users may

[5] NIST Special Publication 800-53, Revision 5, Security and Privacy Controls for Information Systems and Organizations

think they need to do them in sequential order. For example, you must first identify before you document something, and these tasks are listed in reverse order.

- PT2 took a modular approach to this. They did not say that a particular Knowledge Statement was mapped to a specific task.

Project Team 1 (PT1): Risk Assessment (ID.RA-P) Approach

Lisa McKee, PT1 1 Co-Lead, noted that PT1 took a different approach to drafting the TKS statements. The team made a point of building out associations among the statements. The statements are in sequential order. Lisa noted that listing them in alphabetical order may make it harder to piece things together.

Dylan pointed out that in PT1, TKS Statements are grouped together by association. The PWWG is going to have to determine how to capture that in the final work product.

B. PWWG CO-CHAIRS TKS STATEMENT REVIEW UPDATE

PWWG Co-Chairs will meet on **Thursday, April 14th** to review the PT1 TKS statements from ID.RA-P (Risk Assessment) Subcategories ID.RA-P4 and ID.RA-P5. Subcategory ID.RA-P2 will be reviewed last. The NIST Privacy team is coordinating with the NIST AI team on the AI related TKS statements.

III. PROJECT TEAM UPDATES

A. PROJECT TEAM 1: RISK ASSESSMENT ACTIVITIES

Risk Assessment (ID.RA-P): *The organization understands the privacy risks to individuals and how such privacy risks may create follow-on impacts on organizational operations, including mission, functions, other risk management priorities (e.g., compliance, financial), reputation, workforce, and culture.*

Project Team Co-Lead, Lauren Jones, Privacy Counsel, Surescripts, LLC, gave an update on the work of Project Team 1 TKS Statements. The work of the team is almost finished with the team having completed drafting TKS statements for all Subcategories, ID.RA-P1 through ID.RA-P5. The Co-Leads will review the Co-Chairs feedback to share with the team.

Project Team Co-Lead Lisa McKee, Senior Manager Security and Data Privacy, Protiviti, thanked the members of Project Team 1 for their work over the past few months in developing the TKS statements.

Dylan announced that the Co-Chairs comments will be posted to the Project Team 1 Google Drive by tomorrow so that members can come prepared with thoughts on how to address the Co-Chairs comments during next week's PT1 meeting. Team members can also send their feedback via email through the PT1 Google group.

Project Team 1 is no longer accepting new members and encourages the expertise and perspectives of the NIST PWWG membership to participate in the new Project Teams 3 and 4 (see the Join Mailing List Section below).

B. PROJECT TEAM 3: POLICIES, PROCESSES, AND PROCEDURES ACTIVITIES

Governance Policies, Processes, and Procedures (GV.PO-P): *The policies, processes, and procedures to manage and monitor the organization's regulatory, legal, risk, environmental, and operational requirements are understood and inform the management of privacy risk.*

Data Processing Policies, Processes, and Procedures (CT.PO-P): *Policies, processes, and procedures are maintained and used to manage data processing (e.g., purpose, scope, roles and responsibilities in the data processing ecosystem, and management commitment) consistent with the organization's risk strategy to protect individuals' privacy.*

Communication Policies, Processes, and Procedures (CM.PO-P): *Policies, processes, and procedures are maintained and used to increase transparency of the organization's data processing practices (e.g., purpose, scope, roles and responsibilities in the data processing ecosystem, and management commitment) and associated privacy risks.*

Project Team Co-Lead: Dan LoPresto provided a brief update of Project Team 3 activities. The Project Team is currently developing draft TKS Statements for GV.PO-P1: Organizational privacy values and policies (e.g., conditions on data processing such as data uses or retention periods, individuals' prerogatives with respect to data processing) are established and communicated.)

The Project Team 3 Co-Leads continue to encourage the participation, expertise, and perspectives of the NIST PWWG Membership to assist in the development process of the PT3 TKS Statements (see the Join Mailing List Section below).

C. PROJECT TEAM 4: DATA PROCESSING ECOSYSTEM RISK MANAGEMENT ACTIVITIES

Data Processing Ecosystem Risk Management (ID.DE-P): *Data Processing Ecosystem Risk Management (ID.DE-P): The organization's priorities, constraints, risk tolerance, and assumptions are established and used to support risk decisions associated with managing privacy risk and third parties within the data processing ecosystem. The organization has established and implemented the processes to identify, assess, and manage privacy risks within the data processing ecosystem.*

Project Team Co-Lead, Tahir Latif, provided an update on the work of Project Team 4. The Project Team has currently started to develop draft TKS statements for the Subcategory ID.DE-P1 (Data processing ecosystem risk management policies, processes, and procedures are identified, established, assessed, managed, and agreed to by organizational stakeholders).

The Project Team Co-Leads encouraged the participation, expertise, and perspectives of the NIST PWWG Members who are currently in the field of developing privacy programs to assist in the development process of the TKS Statements by joining the bi-weekly meetings.

Project Team 4 is currently open for all who are interested in participating (see the Join Mailing List Section below).

IV. RESOURCES DISCUSSION

Co-Chair, Dylan Gilbert provided a brief discussion regarding the use of resources within the PWWG TKS Statements Mapping documents. Several points were raised for future discussion by the PWWG to be held during the May monthly PWWG meeting as noted below.

- Who is the audience for the notes provided as additional information in the TKS mappings? SMBs who need additional guidance? SMEs who need just a quick reference?
- When is a note warranted in the mapping? Is it when there is a parenthetical?
- How will we keep pace with changing technology? If we freeze references in place, they can become outdated.
- Need a methodology, and rules in place to determine when and how to develop resources. What will that look like?
- Would it be an online reference database? How can we do it in a way that is manageable?
- Future conversation to tackle the questions: Should we do this? Is it worth it given the level of effort required?

The NIST PWWG team will email the PWWG members the resource topics to consider in preparation for the discussion during the May PWWG Monthly meeting.

V. Q & A

N/A

VI. NEXT STEPS & UPCOMING MEETINGS

A. NEXT STEPS

- Project Teams 3 and 4 will continue to review, refine, and finalize TKS Statements and submit to the Co-Chairs for review and comment.
- Project Team 1 will continue to review the Co-Chair feedback as they work to finalize the ID.RA-P TKS statements.
- Co-Chairs will continue to review TKS Statements and will provide feedback to the Project Teams to discuss and provide a consensus.
- 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.

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 1: Risk Assessment (ID.RA-P)

- Thursday, May 5, 2022 | 11:00 a.m. - 12:00 p.m. EDT
- Wednesday, May 18, 2022 | 5:00 p.m. - 6:00 p.m. EDT

Project Team 3: Policies, Processes, And Procedures (GV.PO-P, CT.PO-P, CM.PO-P)

- Thursday, April 28, 2022 | 1:00 p.m. – 1:00 p.m. EDT
- Thursday, May 12, 2022 | 1:00 p.m. – 1:00 p.m. EDT

Project Team 4: Data Processing Ecosystem Risk Management (ID.DE-P)

- Thursday, May 5, 2022 | 2:00 p.m. - 12:00 p.m. EDT
- Thursday, May 19, 2022 | 2:00 p.m. - 12:00 p.m. EDT

NIST Privacy Workforce Public Working Group

- The NIST PWWG Monthly Meeting is held on the 2nd Wednesday of each month.
- Wednesday, May 11, 2022 |1:00 p.m. – 2:00 p.m. EDT

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. JOIN MAILING LIST

All mailing lists are moderated. Please be reminded to review adhere to the Mailing List Rules that can be found on the NIST Privacy Workforce Working Group website.

- Privacy Workforce Working Group (PWWG): PrivacyWorkforceWG+subscribe@list.nist.gov
- Project Team 1 (PT1): PrivacyWorkforcePT1+subscribe@list.nist.gov
- Project Team 3 (PT3)PrivacyWorkforcePT3+subscribe@list.nist.gov
- Project Team 4 (PT4)PrivacyWorkforcePT4+subscribe@list.nist.gov

E. 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.