

NIST PRIVACY WORKFORCE PUBLIC WORKING GROUP (PWWG)

Co-Chair: Dylan Gilbert, NIST Privacy Policy Advisor

MONTHLY MEETING MINUTES

Wednesday, July 12, 2023

1:00 P.M. ET – 2:00 P.M. ET

I. INTRODUCTION

The 25th meeting of the National Institute of Standards and Technology (NIST) Privacy Workforce Public Working Group (PWWG) convened on Wednesday, July 12th from 1:00 P.M. - 2:00 P.M. ET virtually via Microsoft Teams. There were 48 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 remarked that the work is coming down the home stretch toward completion. Today the group will hear the first updates from the newest project teams (Project Teams 6, 7, and 8).

II. PWWG UPDATE

A. Charter Revisions

Dylan informed the group that revisions have been made to the PWWG Charter. The Charter is available in the [PWWG shared drive](#).

The charter now includes a Code of Conduct. The code states that all members should be respectful of different viewpoints and experiences. Additionally, members are expected to communicate in a professional tone, follow the decision-making process the PWWG has in place, accept and offer constructive criticism, and demonstrate efforts to compromise. Members should only use the PWWG forum for topics related to the PWWG and privacy work. The NIST team can issue warnings for violations of this code.

The charter also required clarification around meeting recordings and transcriptions. NIST neither records nor transcribes PWWG meetings. Recording meetings involves a heavy administrative lift, including a lengthy approval process. Meeting minutes are created to document discussions and progress. The minutes are available on the [PWWG website](#) for all members as well as the public. The PWWG is a public working group, and this is a public meeting. There may be occasions when a member records or transcribes the meeting. Members are encouraged to check out the meeting minutes instead. The minutes are a thorough extrapolation of the meeting discussion. The Charter has been updated with new language around this topic.

B. New Finalized TKS Statements and Compilation Documents

Dylan reported that the compilation documents have been completed. Project Team 3 has approximately 275 new Statements. Project Team 4 has approximately 100 new Statements. Project Team 5 has approximately 75 new Statements. Over 400 Statements were created overall. There are now over 700 Statements created between all six project teams. It is a comprehensive and exciting body of work.

Where are we in terms of the Privacy Framework? The entire Identify-P Function has been completed, which includes the Risk Assessment, Inventory and Mapping, Data Processing Ecosystem Risk Management, and Business Environment categories. These are all foundational activities for privacy risk management. Policies,

Processes, and Procedures were already complete as part of the Govern-P Function. The rest of the Policies, Processes, and Procedures have been filled out with material from the Communicate and Control Functions.

A member inquired about the next steps in the process toward the finality of this work. What additional changes will take place? Dylan informed the group that the changes would take place in two rounds. The first is related to conformity. There are slight variations in similar work. Each project team does things a little differently from the next. Since the first project team started, the PWWG team has had the opportunity to gather lessons learned and create a set of norms around the Statements. The NIST team will review the work thus far and make sure it is consistent. The PWWG team has also been collaborating with the NICE team regarding the NICE Workforce Framework. The PWWG team is using the NICE Workforce Framework TKS model. The PWWG and NICE teams are working together to ensure consistency across the material. These changes will be the first round of changes. The goal is to finish the Task, Knowledge, and Skill Statements by the end of this calendar year. The Statements will then be open to the broader community for comment to ensure a wide representation of feedback.

There will be a baseline set of Knowledge and Skills, and maybe Tasks as well. The baseline set are necessary to achieve the Privacy Framework outcomes and activities a company has prioritized. The Co-Chairs are working on the baseline as the process unfolds. If something is broadly applicable, it will be included in the baseline. As you are reading through these documents, it may appear like something is missing. This may be because it is in the baseline. Some baseline activities, however, may be called out again in the Statements. The baseline will be included in the front matter for this taxonomy.

There will also be dependencies among the final TKS Statements. There are situations where a dependency will need to be signaled to refer to other activities in the Privacy Framework. We need to think through how to signal those dependencies when the documents are finalized.

These compilation documents are in the PWWG [‘Reference Documents’](#) folder and are 508 compliant.

Dylan provided a live preview of the compilation and mapping documents. The compilation document is a giant list. The material is organized in three columns. There is the Statement type (Task, Knowledge, or Skill), the ID number, and the description. The compilation inventory provides the maximum amount of flexibility for someone who is using the taxonomy. An individual or organization can select from this list to build a work role or competency, create a job description, or build a course profile. Note that there is no mapping, no dependencies, no additional information, and no terms are defined. As discussed, these may be added later.

There is also the mapping compilation. Everything will be mapped to the Subcategory level when it is updated to a new version after the conformity mapping. Many teams have mapped Knowledge and Skill Statements to specific Task Statements. Again, the dependencies are not captured here. There is a lot of information to potentially include, but not at this stage. The PWWG will need to decide how to handle it.

The Statements developed by the PWWG have a lot of parentheticals. The NICE Framework does not have parentheticals. Instead, NICE has put that information in an additional column that provides further reference information on a given Task, Knowledge, or Skill Statement. We could do the same or choose to keep the parentheticals. Using parentheticals would be consistent with the way the Privacy Framework is presented. However, we do have the ability to pull out the parentheticals and keep the reference information in a different column for the final version of the taxonomy.

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.

Project Team lead, Dana Garbo, provided the PT6 update. Dana and James are very excited to be co-leading the Risk Management Strategy team. Risk Management Strategy is foundational to the adoption of the Privacy Framework.

Currently working on TKS Statements for GV.RM-P1: Risk management processes are established, managed, and agreed to by organizational stakeholders. Goals for this work period are to continue pre-drafting TKS Statements for GV.RM-P2-P3 (Co-Leads).

There has been a lot of healthy debate and looking at the definitions as they stand. Things are progressing nicely. A consistent question for the team is how much do they want to call out privacy risk strategy?

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 Lead, Ivy Orecchio, provided the PT7 update. The team is currently working on TKS Statements for GV.AT-P1: The workforce is informed and trained on its roles and responsibilities. Goals for this work period: Continue pre-drafting TKS statements for GV.AT-P2 through GV.AT-P4 (Co-Leads).

The team has been following the training development approach of the ADDIE method, which thinks of training more broadly.

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-Leads, Abhinav (Abby) Palia, provided the update. Project Team 8 is focused on Data Processing Management (CT.DM-P) The team is currently working on statements for: CT.DM-P1: Data elements can be accessed for review. Goals for this work period are to continue pre-drafting TKS statements for CT.DM-P2 through CT.DM-P10 (Co-Leads).

A frequent topic of discussion is finding knowledge of what has already been defined and how deep the team should go as far as the Tasks themselves. Another is understanding the mapping of the Knowledge and Task Statements and knowing that some Knowledge Statements can pick up multiple Tasks.

Another topic of debate is the relationship between Tasks and Skills and deciding whether something is better as a Task Statement or a Skill Statement.

IV. Q & A

- Q: A member asked if the inventory documents were for every section of the NIST Privacy Framework that has reached this point so far?
- A: Yes, this is everything that has been done so far.

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)

- Second Meeting: Thursday, July 27, 2023 | 1:00pm – 2:00pm ET

Project Team 7 (PT7)

- Third Meeting: Wednesday, July 19, 2023 | 1:00pm – 2:00pm ET

Project Team 8 (PT8)

- Third Meeting: Thursday, July 20, 2023 | 11:00am – 12:00pm ET

NIST Privacy Workforce Public Working Group

- Wednesday, August 9, 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

RESOURCES:

E-mail addresses for members to join/subscribe: Privacy Workforce Working Group (PWWG): PrivacyWorkforceWG+subscribe@list.nist.gov

Project Team 6 (PT6): PrivacyWorkforcePT6+subscribe@list.nist.gov

Project Team 7 (PT7): PrivacyWorkforcePT7+subscribe@list.nist.gov

Project Team 8 (PT8): PrivacyWorkforcePT8+subscribe@list.nist.gov

PWWG Support: PWWG@nist.gov