# NIST PRIVACY WORKFORCE PUBLIC WORKING GROUP (PWWG)

**Co-Chair:** Dylan Gilbert, NIST Privacy Policy Advisor

**MONTHLY MEETING MINUTES**
**Wednesday, February 14, 2024**
**1:00 P.M. ET – 2:00 P.M. ET**

## I. INTRODUCTION

The 32nd meeting of the National Institute of Standards and Technology (NIST) Privacy Workforce Public Working Group (PWWG) convened on Wednesday, February 14th from 1:00 P.M. - 2:00 P.M. ET virtually via Microsoft Teams. There were 38 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 to the meeting.

## II. PWWG UPDATE

### A. PWWG TIMELINE UPDATE

Dylan discussed the timeline for the work of the final Project Teams and completion of TKS Statements for the remaining Privacy Framework Subcategories. The currently active Project Teams are on a very tight schedule with a target end date of March, 2024.

The NIST Privacy Team's goal is to publish the initial Privacy Workforce Taxonomy Public Draft in April, 2024. There will be a public comment period and then Version 1.0 of the Privacy Workforce Taxonomy will be published in the summer of 2024. This has been a long process, almost three years, and there is still a lot of work to be done to get to get to the publication of the Privacy Workforce Taxonomy.

### B. TKS COMPILATION DOCUMENTS UPDATE

Dylan announced that Version 7.0 of the TKS Compilation Inventory and Mapping documents are now available in the PWWG Reference Documents folder on the PWWG Google Drive. This latest version contains the TKS Statements for the Awareness and Training Subcategories (GV.AT-P) completed by Project Team 7. There are currently more than 700 TKS Statements, a number which will likely grow to more than 1,000 when it is complete.

The TKS Compilation Inventory is an alphabetical list of all the TKS Statements to provide maximum flexibility for those using the taxonomy. Organizations can consult the TKS Inventory, and choose Tasks, Knowledge, and Skill Statements that are relevant to their organization as they build out a work role or a job listing, for example. The TKS Mapping contains the TKS Statements mapped to the individual Subcategories in the NIST Privacy Framework.

Dylan noted that there is also a TKS Baseline inventory which he is currently reviewing to make sure that the baseline statements are broadly applicable across the Privacy Framework. He has also been consulting with NIST colleagues in the National Initiative for Cybersecurity Education (NICE) program that have ownership over the NICE Workforce Framework for Cybersecurity (NICE Framework). Many of the NICE Framework Skills could be applicable to the Privacy Framework Workforce Taxonomy.

Dylan encouraged members to think about what would make the final Taxonomy most useful to them and their organizations, and if they have suggestions, to share that with the PWWG team, at pwwg@nist.gov.

### C. PWWG FUTURE WORK

Dylan asked attendees to think about what the future of the PWWG should be. The Project Teams are almost done with their work. Should NIST call it a day once the Taxonomy is published? Some members have expressed a desire to continue meeting monthly to tackle 'Phase 2' of this endeavor.

One example of work that the PWWG could focus on is to put together sample work roles. There is a lot of debate over what a Privacy Engineer and a Privacy Architect are and the difference between them. The PWWG could help provide examples of the tasks, knowledge, and skills associated with a given work role.

Another example would be to use the Taxonomy to build out a high-level privacy competency -- a baseline level of privacy expertise. These are things that organizations may need within their workforce to ensure that they are sufficiently skilled to handle privacy and risk management.

Another option for the focus of future PWWG meetings is to spin up sector-specific privacy Communities of Interest (COI), such as a Healthcare sector COI, to work on next steps with the Privacy Taxonomy within the particular sector.

The NIST PWWG Team will send out a Google Form to members via the PWWG Google Group to solicit input from the PWWG and the results will be discussed during the March 13 PWWG meeting.

## III. PROJECT TEAM UPDATES

### A. PROJECT TEAM LEAD APPRECIATION

Dylan announced that Project Team 6 (PT6) and Project Team 8 (PT8) have completed their work on drafting TKS Statements for the Risk Management Strategy Category in the Govern Function (PT6) and the Data Processing Management Category in the Control Function. Dylan thanked PT6 Co-Leads, Dana Garbo, and James Koons and PT8 Co-Leads, Abhinav Palia, Nikita Samarin, and Ridwan Badmus, for their efforts in leading these Project Teams. He also thanked the members who participated in the Project Team meetings and shared their expertise.

Dylan noted that the Co-Leads are just finishing up the final details of the TKS Statements and those will be added to the next version of the TKS Compilation and Mapping documents.

### B. UPDATE OF PROJECT TEAM 9: DATA PROCESSING AWARENESS (CM.AW-P)

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

- **Data Processing Awareness (CM.AW-P):** Individuals and organizations have reliable knowledge about data processing practices and associated privacy risks, and effective mechanisms are used and maintained to increase predictability consistent with the organization's risk strategy to protect individuals' privacy.
    - **CM.AW-P1:** Mechanisms (e.g., notices, internal or public reports) for communicating data processing purposes, practices, associated privacy risks, and options for enabling individuals' data processing preferences and requests are established and in place.
    - **CM.AW-P2:** Mechanisms for obtaining feedback from individuals (e.g., surveys or focus groups) about data processing and associated privacy risks are established and in place.
    - **CM.AW-P3:** System/product/service design enables data processing visibility.

- **CM.AW-P4:** Records of data disclosures and sharing are maintained and can be accessed for review or transmission/disclosure.
- **CM.AW-P5:** Data corrections or deletions can be communicated to individuals or organizations (e.g., data sources) in the data processing ecosystem.
- **CM.AW-P6:** Data provenance and lineage are maintained and can be accessed for review or transmission/disclosure.
- **CM.AW-P7:** Impacted individuals and organizations are notified about a privacy breach or event.
- **CM.AW-P8:** Individuals are provided with mitigation mechanisms (e.g., credit monitoring, consent withdrawal, data alteration or deletion) to address impacts of problematic data actions.

Dylan gave the update for PT9. There are eight Subcategories in the Data Processing Awareness Category. Paul Lanois, Stuart Lee, and Shoshana Rosenberg are the Project Team Co-Leads, and are working on TKS Statements around transparency outcomes, visibility into the organization's data processing, and how to communicate the data processing activities. They have completed Subcategory CM.AW-P and are moving on to CM.AW-P5 next week.

**C. UPDATE OF PROJECT TEAM 10: MONITORING AND REVIEW (GV.MT-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.

- **Monitoring and Review (GV.MT-P):** The policies, processes, and procedures for ongoing review of the organization's privacy posture are understood and inform the management of privacy risk.

    - **GV.MT-P1:** Privacy risk is re-evaluated on an ongoing basis and as key factors, including the organization's business environment (e.g., introduction of new technologies), governance (e.g., legal obligations, risk tolerance), data processing, and systems/products/services change.
    - **GV.MT-P2:** Privacy values, policies, and training are reviewed and any updates are communicated.
    - **GV.MT-P3:** Policies, processes, and procedures for assessing compliance with legal requirements and privacy policies are established and in place.
    - **GV.MT-P4:** Policies, processes, and procedures for communicating progress on managing privacy risks are established and in place.
    - **GV.MT-P5:** Policies, processes, and procedures are established and in place to receive, analyze, and respond to problematic data actions disclosed to the organization from internal and external sources (e.g., internal discovery, privacy researchers, professional events).
    - **GV.MT-P6:** Policies, processes, and procedures incorporate lessons learned from problematic data actions.
    - **GV.MT-P7:** Policies, processes, and procedures for receiving, tracking, and responding to complaints, concerns, and questions from individuals about organizational privacy practices are established and in place.

Project Team 10 (PT10) Co-Leads Catherine Tomasi gave the update for PT10. Catherine noted that PT10 has been able to leverage some of the work done by previous Project Teams. PT10 is finishing up Subcategory GV.MT-P3 and expects that once they receive the feedback from the Co-Chairs, they will be able to replicate these TKS in the remaining Subcategories.

**C. UPDATE OF PROJECT TEAM 11: DISASSOCIATED PROCESSING**

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

- **Disassociated Processing (CT.DP-P):** Data processing solutions increase disassociability consistent with the organization's risk strategy to protect individuals' privacy and enable implementation of privacy principles (e.g., data minimization).

    - **CT.DP-P1**: Data are processed to limit observability and linkability (e.g., data actions take place on local devices, privacy-preserving cryptography).
    - **CT.DP-P2**: Data are processed to limit the identification of individuals (e.g., de-identification privacy techniques, tokenization).
    - **CT.DP-P3**: Data are processed to limit the formulation of inferences about individuals' behavior or activities (e.g., data processing is decentralized, distributed architectures).
    - **CT.DP-P4**: System or device configurations permit selective collection or disclosure of data elements.
    - **CT.DP-P5**: Attribute references are substituted for attribute values.

Project Team 11 (PT11) Co-Leads Dr. Sarah Lewis Cortes and Hank Roser gave the update for PT11. There are 5 Subcategories in PT11. They have completed CT.DP-P1 and the TKS Statements have been reviewed by the PWWG Co-Chairs. The feedback from the Co-Chairs will help to inform Subcategories CT.DP-P2 and CT.DP-P3. PT11 has also completed TKS Statements for CT.DP-P5 and is awaiting the Co-Chair feedback.

## IV. Q & A

Question from Chat: "Thoughts on providing guidance in the Ad Tech world?"

- Dylan responded that this may be an example of a good use of a COI. If there are ad technology stakeholders that want to draft work roles or competencies that could be an option for continuation of the PWWG work.

## V. NEXT STEPS & UPCOMING MEETINGS

### A. 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 9 (PT9)**

- Biweekly Meeting: Thursday, February 22, 2024 | 2:00pm – 3:00pm ET

**Project Team 10 (PT10)**

- Weekly Meeting: Wednesday, February 14, 2024 | 2:00pm – 3:00 pm ET

**Project Team 11 (PT11)**

- Biweekly Meeting: Tuesday, February 20, 2024 | 1:00pm – 2:00pm ET

**NIST Privacy Workforce Public Working Group**

- Wednesday, March 13, 2024 | 1:00pm – 2:00pm ET

### B. 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.

### C. 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.

**D. 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
- PT9 (CM.AW-P): PrivacyWorkforcePT9+subscribe@list.nist.gov
- PT10 (GV.MT-P): PrivacyWorkforcePT10+subscribe@list.nist.gov
- PT11 (CT.DP-P): PrivacyWorkforcePT11+subscribe@list.nist.gov