# NIST PRIVACY WORKFORCE PUBLIC WORKING GROUP (PWWG)

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

**MONTHLY MEETING MINUTES**
**Wednesday, March 13, 2024**
**1:00 P.M. ET – 2:00 P.M. ET**

## I. INTRODUCTION

The 33rd meeting of the National Institute of Standards and Technology (NIST) Privacy Workforce Public Working Group (PWWG) convened on Wednesday, March 13th from 1:00 P.M. - 2:00 P.M. ET virtually via Microsoft Teams. There were 31 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. PROJECT TEAM UPDATES

### A. 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.

    1. **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.
    2. **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.
    3. **CM.AW-P3:** System/product/service design enables data processing visibility.
    4. **CM.AW-P4:** Records of data disclosures and sharing are maintained and can be accessed for review or transmission/disclosure.
    5. **CM.AW-P5:** Data corrections or deletions can be communicated to individuals or organizations (e.g., data sources) in the data processing ecosystem.
    6. **CM.AW-P6:** Data provenance and lineage are maintained and can be accessed for review or transmission/disclosure.
    7. **CM.AW-P7:** Impacted individuals and organizations are notified about a privacy breach or event.
    8. **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 provided the update for PT9. There were no similarities in the Subcategory to leverage making the work a very heavy lift. There are eight Subcategories in the Data Processing Awareness Category. The Co-Chairs are reviewing CM.AW-P4 and CM.AW-P5 tomorrow as well as potentially CM.AW-P6. The team will finish their last two subcategories this week. Dylan thanked the PT9 team members for all their hard work.

PT9 members were reminded to keep an eye out for information about future meetings should they be necessary.

## B. 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-Lead, Phil Lowry, gave the update for PT10. Phil noted that GV.MT-P1 through GV.MT-P3 had a slow start given the learning curve. The team has populated and vetted the Task, Knowledge, and Skill Statements for GV.MT-P1 through GV.MT-P3. They do have provisional levels for GV.MT-P4 through GV.MT-P7. They have culled Statements from the Baseline and the current compilation and adapted them to this Subcategory. The team will begin reviewing the Statements for P4-P7 during their meeting today. P4-P7 are similar in their analytical construct. They are not the same but talk about communicating policies, processes, and procedures. They talk about having appropriate responses for problematic data actions as well as having appropriate policies, processes, and procedures. They are all inter-related in that the analytical pieces are similar. PT10 is on track to wrapping up in the next week.

Dylan thanked the members for all their work. The team is in good shape.

## 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-Lead, Dr. Sarah Lewis Cortes, provided the update for PT11. There are 5 Subcategories in PT11, and the team has made great progress on all of them. It is a very technical area and some of them were high level. They first teased out the original meaning and areas of control that they were intended to cover. A lot of progress was made on the suggested changes for the Statements.

Dylan noted that like Project Team 10, the first three Subcategories of CT.DP-P are variations on a theme which they have leveraged in their work. Dylan is meeting with the Team leads at the end of the week to finish Statements for CT.DP-P1 through CT.DP-P3 as well as CT.DP-P5. There was some lively debate around CT.DP-P4. The team decided to provide a few different options for the Co-Chairs to review. The team is almost finished with this very technical Subcategory.

The PT11 members will be notified about the status of their next meeting.

## III. PWWG UPDATES

### A. TIMELINE TO COMPLETION

We are at the end of the road with this work. It will be three years between the start and putting together the final Privacy Workforce Taxonomy Public Draft. The draft will be completed by the end of March. It will then be opened for a public comment period when the public draft becomes available.

What will this look like? It is always subject to change, but in general it will be a very online centric environment for the Public Draft. The IPD and template to provide public comments will be available for download from the NIST Privacy Framework website. In the IPD, you will find the mapping document maintained throughout this process. The mapping document will include General Task, Knowledge, and Skill (TKS) Statements (formerly known as the Baseline). There are approximately twelve General TKS Statements in total that are applicable throughout the Privacy Framework. The final compilation will include about one thousand Task, Knowledge, and Skill Statements.

We hope everyone will provide their comments. The PWWG Team is open to all suggestions. If there is something anyone believes should be removed, please let us know within your comment. If there is anything we missed within the project teams and needs to be added to the Subcategory Mapping or to the General Baseline set of TKS Statements, please offer those thoughts as well. Or if there are any general tweaks or revisions to the current TKS Statements please let us know with rational for why it should change.

The website will provide additional information on the Taxonomy. There will be information on the background and where it came from. The majority of this has been the product of this working group but the work goes all the way back to the development of the NIST Privacy Framework and putting workforce as a key topic within the NIST Privacy Framework roadmap. All the information will be available for anyone who would like to learn about the journey to the taxonomy.

Reference resources will be available on the website, such as the TKS Authoring Guide, as well as any other helpful resources. A public announcement will be made about the public comment period. The announcement will include information about what NIST is hoping to get with respect to comments, information about deadlines, and other information of that nature will be included as well. Stay tuned!

## IV. OPEN DISCUSSION

### A. FUTURE WORK

Where do we go from here? There have been eleven project teams that have worked over the course of three years to create our taxonomy, which has been a great endeavor. The NIST Team feels that it has been an appropriate vehicle to create this taxonomy, leveraging the PWWG members' collective expertise. We achieved our goal to identify and document Task, Knowledge, and Skills in alignment with the NIST Privacy Framework. There are, however, more things we can do with this working group.

Ahead of today's meeting the NIST team sent out a poll and asked what members think should be done moving forward. There were thirty-five responses to the poll. Most of the responses were that the work of this group should continue. The poll included the following choices:

1. Creating example work roles.
   - Think of a notional work role and leverage the TKS Statements we have created and think about what can be bundled together to create a work role.
2. Creating privacy competency
   - If we want to upskill our workforce, it may not be as simple as hiring a privacy specific person, but maybe we can provide a privacy competency that has a bundle of TKS that may be aligned with the workforce generally or are domain specific, maybe that could be helpful to organizations looking to upskill or train folks they already have that need to have more competency around privacy or privacy risk management.
3. Communities of Interest (public working group):
   - A little less than half of the responses were interested in a community of interest. This could be sector-specific, for example.
4. Other responses included:
   - Creating a certification process comparable to ISO 27701
     - NIST does not do certifications, so this is unlikely.
   - Update TKS to PF1.1. Tie knowledge and skills as informative reference to 800-50 rev 1
     - Once 1.1 is released there will be an immediate misalignment. A reasonable effort within this group would be updating the taxonomy and/or tying knowledge and skills as an informative reference to 800-50 Rev 1
   - Intersection of AI and Privacy
     - There are a couple AI flavored subcategories within the Privacy Framework. There may be ways to consider going further with the material we have.
   - Privacy in new and emerging technologies
     - AI, IoT, quantum computing, etc.

Dylan opened the meeting to members for discussion. He first read the initial chat comments:

- I liked working with this group and I would be open to continue the relationships in any of those topics. They are all relevant to what we are doing in Texas and where I work.
- I just recently joined the group, and this is my first meeting so forgive me if this is out of scope or already covered. I am curious about Privacy Impact Assessments and Risk Ratings. Would additional work in those areas be feasible?

    - Dylan suggested that the member look at the Risk Assessment Category. There are a lot of Task, Knowledge, and Skills that are around doing a privacy risk assessment of which a privacy impact assessment or risk rating would fall underneath that general umbrella. If there is more work to do to dig into more detail on that it is a reasonable option.
- Good afternoon! I am open and interested in continuing. I am interested in helping with the influence of privacy in the financial industry.

A member noted that there are a lot of job descriptions that are not well written. They are written by HR or other folks who are not familiar with what is involved in privacy. Compiling the Task, Knowledge, and Skill Statements into job descriptions will help standardize the job descriptions. It would also help organizations not only pick roles for their privacy program but also in putting out job descriptions. Second, on competencies, as someone from a company that conducts training, they would like to see good high-quality Knowledge and Skill Statements to which they can potentially train. The knowledge can be applied to a job role that fits a job role and/or enhances their knowledge and skills to potentially get jobs in the future. Dylan noted that the member views the work roles and competencies as travelling in pairs because of the synergies between them.

Another member underscored the previous comment about core competencies and how it relates to hiring individuals. If they could map a role to a Task, Knowledge, or Skill it would be very useful especially for those that do not have a lot of exposure to privacy.

Dylan read another comment from the chat. The member hopes the work of the PWWG continues and has a particular interest in the influence of privacy in the financial industry. Dylan noted that this could be a community of interest (COI) for the financial sector.

Another comment from the chat noted that some companies think privacy is an item to be checked off.

A member commented about their interest in a community of interest as well as creating privacy competencies. A community of interest would allow members to be among privacy professionals who collaborate and share an interest in furthering privacy as a career. Dylan noted that members have enjoyed the opportunity to collaborate and network while doing this work.

PT6 Team Lead, Dana Garbo, noted how essential the training piece will be. Focus the next phase on taking all the work conducted over the last three years and turn it into actionable training and awareness to better inform and upscale the workforce. It would be great to get members together in person to work this information out. Dylan noted that there will be several opportunities this year, both formally and informally, to get together. NIST will be hosting a workshop on the NIST Privacy Framework Version 1.1 in the Data Governance Profile later this year. A public announcement about the workshop will be made soon. Dylan noted that various organizations will be holding events that members could informally get together around as well.

A member expressed concern about communities of interest. Unless you have a task in hand, like developing work roles, the community of interest will lose steam. It will not materialize without some goal in hand.

The PWWG will hold a meeting in April. Dylan will provide an overview of the Privacy Workforce Taxonomy Public Draft, answer questions, and publicly thank the final three teams' leads for all their hard work. Where we go beyond that will be subject to how we decide to structure a Phase II for future work this year. The public draft will be available prior to the April meeting.

## V. Q & A

## VI. NEXT STEPS & UPCOMING MEETINGS

### A. UPCOMING MEETINGS

The work is nearly finished. There may be some ad-hoc meetings with respect to Project Teams 10 and 11 over the next week, if necessary, to finish the material. Project Team 9 will meet tomorrow at 2:00pm.

The PWWG will meet in April to discuss the initial public taxonomy. Future monthly meetings are to be determined based on what is decided for Phase 2. If anyone has thoughts about how to proceed in the future, please send an email to the PWWG box.

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.

**NIST Privacy Workforce Public Working Group**

- Wednesday, April 10, 2024 | 1:00pm – 2:00pm ET

## VII. 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.

## VIII. 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.

## IX. 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