NIST PRIVACY WORKFORCE PUBLIC WORKING GROUP (PWWG)

Co-Chair: Mary Chaney, Managing Attorney, The Law Offices of Mary N. Chaney, PLLC

MEETING MINUTES

Wednesday, September 14, 2022
1:00 p.m. – 2:00 p.m. EDT

I. INTRODUCTION

The 17th meeting of the National Institute of Standards and Technology (NIST) Privacy Workforce Public Working Group (PWWG) convened on Wednesday, September 14th, 2022 from 1:00 P.M. - 2:00 P.M. EDT virtually via Microsoft Teams. There were 60 members on the call.

The PWWG provides a forum for participants from the general 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[1] and the National Initiative for Cybersecurity Education (NICE) Workforce Framework for Cybersecurity[2].

PWWG Co-Chair, Mary Chaney, welcomed the members and Project Teams Co-Leads and thanked them for their participation.

II. PWWG UPDATES

PROJECT TEAM 1: RISK ASSESSMENT - FINAL TKS STATEMENTS

Mary announced that the work of Project Team 1 (PT1) is now complete. PT1 focused on the Risk Assessment Category of the Identify Function (ID-RA-P). Mary thanked the PT1 Co-Chairs and all of the team members who worked on this endeavor for over a year, contributing approximately 200 TKS Statements.

The PT1 Risk Assessment (ID.RA-P) TKS Statements have been posted on the PWWG Google drive in the "Reference Documents" folder for PWWG members to view. These TKS Statements have been combined with the TKS Statements from the Inventory and Mapping Category (ID.IM-P) of the Identify Function that was the work of Project Team 2 (PT2). The folder contains two TKS documents: a TKS Inventory document which contains an alphabetized list of approved TKS Statements; and a TKS Mapping document which maps TKS Statements to the Privacy Framework Core Subcategories.

Mary noted that while these TKS Statements are final for now, the entire body of PWWG TKS Statements will be subject to another round of comments and feedback from PWWG members and Project Team members when all of the Project Teams have completed their work.

As each of the Project Teams completes their work, their assigned Category's TKS Statements will be

[1] https://www.nist.gov/privacy-framework/privacy-framework
[2] https://www.nist.gov/itl/applied-cybersecurity/nice/nice-framework-resource-center

combined with those of other teams in a single inventory document. When the TKS Inventory is complete, organizations can use this document in a number of ways such as to build work roles, teams, and competencies or to create job descriptions.

III. PROJECT TEAM UPDATES

A. PROJECT TEAM 1: RISK ASSESSMENT (ID.RA-P) ACTIVITIES

Category - 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.
Subcategories (5):

- **ID.RA-P1**: Contextual factors related to the systems/products/services and the data actions are identified (e.g., individuals' demographics and privacy interests or perceptions, data sensitivity and/or types, visibility of data processing to individuals and third parties).
- **ID.RA-P2**: Data analytic inputs and outputs are identified and evaluated for bias.
- **ID.RA-P3**: Potential problematic data actions and associated problems are identified.
- **ID.RA-P4**: Problematic data actions, likelihoods, and impacts are used to determine and prioritize risk.
- **ID.RA-P5**: Risk responses are identified, prioritized, and implemented.

PT1 TKS Taxonomy Mapping
PT1 Co-Lead, Lisa McKee, Director of Governance, Risk, Compliance and Privacy, Hudl, and Lauren Jones, Privacy Counsel, Surescripts, LLC, gave a readout of the work of PT1 that they are now wrapping up. The Co-Leads noted that the work of this team was an enormous undertaking and being the first Project Team made it extra challenging, with no existing TKS Statements or Inventory to reference.

Lisa and Lauren are currently finishing up a mapping of the new TKS Statements in the TKS Inventory and TKS Mapping documents with their final PT1 Risk Management TKS Workbook. Lisa noted that she and Lauren feel passionately about mapping these back to the working document so there is a record. They walked through their Excel document with the PWWG attendees showing the alignment between their Task, Knowledge, and Skill Statements while referring back to the new TKS Inventory and TKS Mapping documents.

Lisa noted that during the PT1 TKS drafting process the TKS Statements were developed in groupings with Knowledge and Skill Statements aligned to specific Task Statements. It was the intent of the Co-Leads that the TKS Statements would continue to be aligned. The consolidated TKS Inventory and Mapping documents list the TKS Statements sequentially. In the Inventory document they are listed in alphabetical order while in the Mapping document they are listed by Subcategory. The TKS Statements in the TKS Inventory document do not map back to any particular Subcategory.

Lisa noted that the Excel TKS Workbook will be available to view on the PWWG Google Drive once the Co-Leads have completed their mapping to the new TKS Inventory and TKS Mapping documents.

Lisa and Lauren thanked the Project Team 1 members who worked hard over a long period of time to complete the Risk Assessment TKS Statements.

B. PROJECT TEAM 3: POLICIES, PROCESSES, AND PROCEDURES (GV.PO-P, CT.PO-P, CM.PO-P)

Project Team 3 (PT3) is working on drafting TKS Statements for three Policies, Processes, and Procedures Categories comprising a total of twelve Subcategories from three separate Functions: Govern (GV-P); Control (CT-P); and Communicate (CM-P).

Category 1 - 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.
Subcategories (6):

- **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.
- **GV.PO-P2:** Processes to instill organizational privacy values within system/product/service development and operations are established and in place.
- **GV.PO-P3:** Roles and responsibilities for the workforce are established with respect to privacy.
- **GV.PO-P4:** Privacy roles and responsibilities are coordinated and aligned with third-party stakeholders (e.g., service providers, customers, partners).
- **GV.PO-P5:** Legal, regulatory, and contractual requirements regarding privacy are understood and managed.
- **GV.PO-P6:** Governance and risk management policies, processes, and procedures address privacy risks.

Category 2 - 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.
Subcategories (4):

- **CT.PO-P1:** Policies, processes, and procedures for authorizing data processing (e.g., organizational decisions, individual consent), revoking authorizations, and maintaining authorizations are established and in place.
- **CT.PO-P2:** Policies, processes, and procedures for enabling data review, transfer, sharing or disclosure, alteration, and deletion are established and in place (e.g., to maintain data quality, manage data retention).
- **CT.PO-P3:** Policies, processes, and procedures for enabling individuals' data processing preferences and requests are established and in place.
- **CT.PO-P4**: A data life cycle to manage data is aligned and implemented with the system development life cycle to manage systems.

Category 3 - 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.
Subcategories (2):

- **CM.PO-P1:** Transparency policies, processes, and procedures for communicating data processing purposes, practices, and associated privacy risks are established and in place.

- **CM.PO-P2**: Roles and responsibilities (e.g., public relations) for communicating data processing purposes, practices, and associated privacy risks are established.

PT3 Co-Lead, Alicia Christensen, VP, General Counsel, Chief Compliance Officer at National Jewish Health, gave an update on the work of PT3. The team submitted the first draft of TKS Statements for Category GV.PO-P to the PWWG Co-Chairs for their review and received feedback on Subcategories GV.PO-P1 through GV-PO-P4. They are awaiting comments on the remaining Subcategories, GV.PO-P5 and GV.PO-P6.

PT3 is currently working on discussing the PWWG Co-Chairs recommendations and refining their TKS Statements during their biweekly meetings. The team has completed review of GV.PO-P1 and is working on GV.PO-P2. Once the GV.PO-P Subcategories review is complete they will continue work on drafting TKS Statements for Data Processing Policies, Processes, and Procedures (CT.PO-P) Subcategories.

The Project Team 3 Co-Leads continue to encourage the participation, expertise, and perspectives of the larger NIST PWWG Membership to assist in the development process of the PT3 TKS Statements. They welcome more members to join the team. (See the Join Mailing List Section below).

C. PROJECT TEAM 4: DATA PROCESSING ECOSYSTEM RISK MANAGEMENT (ID.DE-P) ACTIVITIES

Category - 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.
Subcategories (5):

- **ID.DE-P1**: Data processing ecosystem risk management policies, processes, and procedures are identified, established, assessed, managed, and agreed to by organizational stakeholders.
- **ID.DE-P2:** Data processing ecosystem parties (e.g., service providers, customers, partners, product manufacturers, application developers) are identified, prioritized, and assessed using a privacy risk assessment process.
- **ID.DE-P3:** Contracts with data processing ecosystem parties are used to implement appropriate measures designed to meet the objectives of an organization's privacy program.
- **ID.DE-P4:** Interoperability frameworks or similar multi-party approaches are used to manage data processing ecosystem privacy risks.
- **ID.DE-P5:** Data processing ecosystem parties are routinely assessed using audits, test results, or other forms of evaluations to confirm they are meeting their contractual, interoperability framework, or other obligations.

Project Team 4 (PT4) Co-Leads, Paul Lanois, Director, Fieldfisher, Tahir Latif, Head of Practice, Data Protection, Artificial Intelligence and Analytics, Cognizant Worldwide, and Anne Connell, Senior Cybersecurity Engineer, Software Engineering Institute, Carnegie Mellon University gave the update for PT4.

PT4 has had 14 meetings to date and the team recently completed their first draft of TKS Statements for Subcategory ID.DE-P2. The PWWG Co-Chairs completed a preliminary walkthrough of those TKS Statements. The PT4 Co-Leads plan to discuss the feedback and refine the TKS Statements before resubmitting the PWWG Co-Chairs for a more thorough review. PT4 will continue to draft TKS

Statements for the remaining ID.DE-P Subcategories.

Anne noted that PT4 is still welcoming new members and encouraged anyone who is interested to join the team and offer their expertise. The team is particularly interested in hearing from those practitioners who are implementing the Privacy Framework. (See the Join Mailing List Section below).

D. PROJECT TEAM 5: BUSINESS ENVIRONMENT (ID-BE-P) ACTIVITIES

Category - Business Environment (ID.BE-P): The organization's mission, objectives, stakeholders, and activities are understood and prioritized; this information is used to inform privacy roles, responsibilities, and risk management decisions.
Subcategories:

- **ID.BE-P1**: The organization's role(s) in the data processing ecosystem are identified and communicated.
- **ID.BE-P2**: Priorities for organizational mission, objectives, and activities are established and communicated.
- **ID.BE-P3**: Systems/products/services that support organizational priorities are identified and key requirements communicated.

Project Team 5 (PT5) Co-Lead Brandi Bennet, Data Privacy and Security Attorney gave a status update for PT5. This is the newest Project Team and has now met three times. The team is currently drafting TKS Statements for Subcategory ID.BE-P1. The team met earlier in the week, and the Co-Leads were happy to welcome some new members on the call. Brandi noted that they have found that some of the team's work is redundant because they can piggyback on work that has already been completed by other Project Teams and they are able to reference existing TKS Statements.

The PT5 Co-Leads are still hoping to add more members. As the newest team it currently has the smallest number of members. Brandi asked any members of Project Teams that have just wrapped up to consider joining PT5 to share their expertise. Any member of the PWWG who would like to contribute is also encouraged to join. (See the Join Mailing List Section below).

IV. Q & A

Q. How do I get involved?
A. Consider joining one or more Project Teams. Check out the PWWG website for meeting schedules and information on how to sign up.

Q. Is there a description of the Teams?
A. There is a description of existing Project Teams on the PWWG website.

V. NEXT STEPS & UPCOMING MEETINGS

Mary thanked everyone for joining the meeting and for their patience with the earlier technical issues on the call. Attendees were encouraged to consider joining existing Project Teams to offer their expertise.

A. NEXT STEPS

- Project Teams 3, 4, and 5 will continue to draft, refine, and finalize TKS Statements and submit to the Co-Chairs for review and comment.
- Project Team 1 will complete their mapping of the TKS Inventory to their TKS Taxonomy for ID.RA-P and post this on the PWWG Google Drive.
- PWWG Co-Chairs will continue to review TKS Statements and 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) – no further meetings.

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

- Thursday, September 15, 2022 | 1:00 p.m. – 2:00 p.m. EDT
- Thursday, September 29, 2022 | 1:00 p.m. – 2:00 p.m. EDT

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

- Thursday, September 15, 2022 | 2:00 p.m. – 3:00 p.m. EDT
- Thursday, September 29, 2022 | 2:00 p.m. – 3:00 p.m. EDT – additional meeting
- Thursday, October 6, 2022 | 2:00 p.m. – 3:00 p.m. EDT

Project Team 5: Business Environment (ID.BE-P)

- Tuesday, September 27 | 1:00 p.m. – 2:00 p.m. EDT
- Tuesday, October 11 | 1:00 p.m. – 2:00 p.m. EDT

NIST Privacy Workforce Public Working Group

- The NIST PWWG Monthly Meeting is the 2nd Wednesday of each month.
- Wednesday, October 12, 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

In order 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
- Project Team 3 (PT3): PrivacyWorkforcePT3+subscribe@list.nist.gov

- Project Team 4 (PT4): PrivacyWorkforcePT4+subscribe@list.nist.gov
- Project Team 5 (PT5): PrivacyWorkforcePT5+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.