NIST PRIVACY WORKFORCE PUBLIC WORKING GROUP (PWWG)

Co-Chair: Melanie Ensign, Founder & CEO, Discernable, Inc.

MEETING MINUTES

Wednesday, November 9, 2022
1:00 p.m. ET – 2:00 p.m. ET

I. INTRODUCTION

The 19th meeting of the National Institute of Standards and Technology (NIST) Privacy Workforce Public Working Group (PWWG) convened on Wednesday, November 9th, 2022 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 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, Melanie Ensign, welcomed attendees and Project Team Co-Leads and thanked them for their participation.

II. PWWG UPDATES

PWWG CO-CHAIR UPDATE

Melanie announced that PWWG Co-Chair, Trevor Hughes, is stepping down from the PWWG. She thanked Trevor for serving in this role since the PWWG began in May 2021. Melanie introduced the new PWWG Co-Chair, Doug Forman, Certification Director, International Association of Privacy Professionals (IAPP). Doug will join Melanie and fellow Co-Chair Mary Chaney in reviewing TKS Statements drafted by the Project Teams and providing feedback.

COMPLETED TKS STATEMENTS INVENTORY

Melanie announced that the NIST AI Team is working on reviewing the ID.RA-P2 TKS Statements with a target timeline for completion in January 2023. The NIST AI Team is well positioned to look at this Risk Assessment Subcategory, ID.RA-P2 (Data analytic inputs and outputs are identified and evaluated for bias). Once these TKS Statements are approved, they will be added to the TKS Inventory documents on the PWWG Google Drive.

Melanie reminded members that the PT1 Risk Assessment (ID.RA-P) and PT2 Inventory and Mapping (ID.IM-P) TKS Statements are available to view on the PWWG Google drive in the "Reference Documents" folder.
There are two PDFs:

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

- Inventory document: An alphabetized list of approved TKS Statements. When 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.
- Mapping document: Maps TKS Statements to the Privacy Framework Core Subcategories.

As each of the Project Teams complete their work, their assigned Category's TKS Statements will be 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 3: POLICIES, PROCESSES, AND PROCEDURES (GV.PO-P, CT.PO-P, CM.PO-P) ACTIVITIES

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, and Principal Advisor, Frame Privacy Group gave an update on the work of PT3. The team is currently reviewing comments received from the PWWG Co-Chairs on the TKS Statements for the Govern Function Subcategory GV.PO-P5. They are awaiting Co-Chairs' comments on the remaining Subcategory, GV.PO-P6.

During the next PT3 meeting, the team will begin drafting TKS Statements for Data Processing Policies, Processes, and Procedures Subcategories in the Control Function (CT.PO-P).

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).

B. 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-Lead, Paul Lanois, Director, Fieldfisher, gave the team update for PT4. The team is awaiting Co-Chair comments on the draft TKS Statements for Subcategory ID.DE-P2. The PT4 members are nearing completion of draft TKS Statements for ID.DE-P1. The team expects to submit the ID.DE-P1 TKS Statements for next month's PWWG Co-Chair Review meeting. PT4 will begin working on Subcategory, ID.DE-P3 at their next meeting.

PT4 is still open to new members. The team is particularly interested in hearing from those practitioners who have experience in implementing the Privacy Framework. (See the Join Mailing List Section below).

C. 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) recently completed draft TKS Statements for Subcategory ID.BE-P1 and have submitted them for PWWG Co-Chair review. The team has begun drafting TKS Statements for Subcategory ID.BE-P2.

PT5 has struggled with participation on the biweekly calls. This team has the fewest registered members, and the Co-Leads would welcome more voices to share their expertise. (See the Join Mailing List Section below).

IV. NIST CYBERSECURITY INSIGHTS BLOG – OPEN DISCUSSION

Why Employers Should Embrace Competency-Based Learning in Cybersecurity - October 25, 2022
By: Marni Baker-Stein, Bridgett Paradise and Rodney Petersen

Melanie invited meeting attendees to share their thoughts on the latest NIST Cybersecurity Insights blog. The link to the blog was sent with the meeting invite to allow PWWG members to pre-read the text.

Melanie recommended that PWWG members read the blog if they hadn't already done so. The NIST PWWG team is curious about how Working Group members think this may apply to privacy and the

work of the PWWG. How do we measure competence in privacy? How do we define the Tasks, Knowledge, and Skills that people need to implement these frameworks? How do we measure those competencies in privacy when there is not an existing degree or educational program that can fully prepare employees for all of these responsibilities?

There was no feedback on the blog from attendees during the meeting, but members were invited to submit their comments at a later time to the pwwg@nist.gov website or to the PWWG Google group mailing list.

V. Q & A

Question: Are the PWWG Co-Chairs still reviewing comments in Dylan Gilbert's absence?
Answer: Yes, the Co-Chairs are meeting regularly to continue the TKS review process.

Question: What level of expertise is required to participate in the groups? I am new to privacy but want to join if possible?
Answer: Melanie suggested that it may be worthwhile to join a Project Team and ask the Co-Leads and members what they are working on, and where they need help. This Taxonomy is designed to be used by people new to privacy, so it is definitely worth checking out as a way to learn more.

One member added a recommendation to anyone who is new to a Project Team to spend time familiarizing themselves with the Privacy Framework itself, which this Privacy Workforce Taxonomy is built upon. There is a very specific glossary of terms used by the Privacy Framework. Even privacy professionals who don't use the same privacy model are not familiar with some of the terms of art used by the Privacy Framework, for example, Problematic Data Actions, Data Processing Ecosystem. The Privacy Framework Core, the Glossary, and several other foundational documents are available on the PWWG Reference Document Google Drive.

VI. NEXT STEPS & UPCOMING MEETINGS

Melanie thanked everyone for joining the meeting and encouraged attendees to consider joining one of the active 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.
- PWWG Co-Chairs will continue to review TKS Statements and provide feedback to the Project Teams to discuss and provide a consensus.
- NIST AI Team will review TKS Statements for ID.RA-P2 for a targeted completion in January 2023.

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

- Thursday, November 10, 2022 | 1:00pm – 2:00pm ET

- Thursday, December 8, 2022 | 1:00 p.m. – 2:00 p.m. ET
- Note: There will be no meetings on November 24th or December 22nd, 2022.

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

- Thursday, November 17, 2022 | 2:00 p.m. – 3:00 p.m. ET
- Thursday, December 1, 2022 | 2:00 p.m. – 3:00 p.m. ET

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

- Tuesday, November 22, 2022| 1:00 p.m. – 2:00 p.m. ET
- Tuesday, December 6, 2022 | 1:00 p.m. – 2:00 p.m. ET

NIST Privacy Workforce Public Working Group

- The NIST PWWG meets on the 2nd Wednesday of each month.
- Note: There will be no meeting of the PWWG in December.
- Next meeting: Wednesday, January 11, 2022 |1:00 p.m. – 2:00 p.m. 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

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