# NIST PRIVACY WORKFORCE PUBLIC WORKING GROUP (PWWG)

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

**MEETING MINUTES**

Wednesday, October 12 , 2022
1:00 p.m. EDT – 2:00 p.m. EDT

## I. INTRODUCTION

The 18th meeting of the National Institute of Standards and Technology (NIST) Privacy Workforce Public Working Group (PWWG) convened on Wednesday, October 12th, 2022 from 1:00 P.M. – 1:25 P.M. EDT virtually via Microsoft Teams. There were 33 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, Melanie Ensign, 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

Melanie announced that the NIST AI Team is working on reviewing the ID.RA-P2 TKS Statements with a target timeline for completion in November. This Risk Assessment Subcategory, ID.RA-P2 (Data analytic inputs and outputs are identified and evaluated for bias) is in the wheelhouse of the NIST AI Team, which is well positioned to look at issues of bias. Once these TKS Statements are approved, they will be added to the TKS Inventory and Mapping 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:

- 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 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 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, Dan LoPresto, VP, Director, Privacy Compliance, University of Central Florida 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 Govern Function Subcategories GV.PO-P1 through GV-PO-P4. They are awaiting comments on the remaining Subcategories, GV.PO-P5 and GV.PO-P6.

Once the GV.PO-P Subcategories review is complete, PT3 will continue work on 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, Anne Connell, Senior Cybersecurity Engineer, Software Engineering

Institute, Carnegie Mellon University gave the update for PT4.

PT4 recently completed their first draft of TKS Statements for Subcategory ID.DE-P2 and received some preliminary feedback from the PWWG Co-Chairs. The PT4 Co-Leads reviewed the recommendations from the Co-Chairs and made some refinements before resubmitting the ID.DE-P2 TKS Statements for a more formal review. The PT4 members are currently finishing up TKS Statements for ID.DE-P1, and they expect to complete this Subcategory In October and move on to ID.DE-P3.

Anne noted that PT4 still welcomes 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).

### 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) Co-Lead Brandi Bennet, Data Privacy and Security Attorney gave a status update for PT5. The team is currently close to completing TKS Statements for Subcategory ID.BE-P1.

Brandi noted that the team has struggled with low turnout on the biweekly calls. This team has the fewest registered members, and the Co-Leads would welcome more voices to share their expertise in drafting these TKS Statements. Brandi noted the ever-changing privacy landscape points to the need for diversity of input and experience in making this effort a success.

Any member of the PWWG who would like to contribute to the Business Environment Project Team is encouraged to join. (See the Join Mailing List Section below).

## IV. Q & A

Question: Will the PWWG Co-Chairs continue to review TKS Statements submitted by the Project Teams while Dylan Gilbert is on leave of absence?
Answer: Melanie responded that the Co-Chairs would continue to meet and provide comments on submitted TKS Statements. Meghan Anderson, NIST Privacy Risk Strategist, will serve as liaison between the Project Teams and the PWWG Co-Chairs in Dylan's absence.

## V. NEXT STEPS & UPCOMING MEETINGS

**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 complete the review of TKS Statements for ID.RA-P2.
- 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 3: Policies, Processes, And Procedures (GV.PO-P, CT.PO-P, CM.PO-P)

- Thursday, October 13, 2022 | 1:00 p.m. – 2:00 p.m. EDT
- Thursday, October 27, 2022 | 1:00 p.m. – 2:00 p.m. EDT

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

- Thursday, October 20, 2022 | 2:00 p.m. – 3:00 p.m. EDT
- Thursday, November 3, 2022 | 2:00 p.m. – 3:00 p.m. EDT

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

- Tuesday, October 25, 2022| 1:00 p.m. – 2:00 p.m. EDT
- Tuesday, November 8, 2022 | 1:00 p.m. – 2:00 p.m. EDT

NIST Privacy Workforce Public Working Group

- The NIST PWWG meets on the 2nd Wednesday of each month.
- Wednesday, November 9, 2022 |1:00 p.m. – 2:00 p.m. EDT
- There will be no meeting of the PWWG in December.

**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