

NIST PRIVACY WORKFORCE PUBLIC WORKING GROUP (PWWG)

Co-Chair: Dylan Gilbert, Privacy Policy Advisor, National Institute of Standards and Technology

MEETING MINUTES

Wednesday, December 8, 2021

1:00 P.M. ET – 2:00 P.M. ET

I. INTRODUCTION

The eighth (8th) meeting of the National Institute of Standards and Technology (NIST) Privacy Workforce Public Working Group (PWWG) convened on Wednesday, December 8, 2021 from 1:00 P.M. ET - 2:00 P.M. ET virtually via Microsoft Teams.

Co-Chair: Dylan Gilbert, Privacy Policy Advisor, NIST, welcomed and thanked the members and Project Teams Leads for their participation. The Co-Chair provided a brief overview of the agenda that included the update of the NIST PWWG Project Team 3, PWWG Co-Chair Review of TKS Statements, IAPP Privacy Security Risk Conference – Roundtable Report, and Project Team updates from Project Team 1: Risk Assessment (ID.RA-P) and Project Team 2: Inventory and Mapping (ID.IM-P).

II. PWWG UPDATES

A. NIST PWWG PROJECT TEAM 3: POLICIES, PROCESSES, AND PROCEDURES

Co-Chair Dylan Gilbert provided a brief update of the development of NIST PWWG Project Team 3: Policies, Processes, and Procedures. The PWWG Co-Chairs decided to combine the three (3) Privacy Framework Functions of 1) GOVERN-P (GV-P), CONTROL-P (CT-P), and COMMUNICATE-P (CM-P) into one (1) Project Team. The team will consist of three (3) Project Team Leads with multidisciplinary experience to lead Project Team 3. This information will also be updated within the NIST PWWG Charter.

Dylan thanked those members who volunteered to participate as a Team Leads and advised that the selection of the Team Leads will be reviewed within the next coming weeks. The Project Team 3 Co-Leads will be announced on the PWWG Monthly Meeting on January 12, 2022. The Project Team 3 Mailing List will also open in January 2022 those interested in participating.

The NIST PWWG Project Team 3: Policies, Processes, and Procedures, will create TKS Statements for the following Privacy Framework Categories and Subcategories:

- **CATEGORY:** 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:**
 - **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:** 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:**
 - **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:** 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:**
 - **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.

B. PWWG CO-CHAIRS TASK, KNOWLEDGE, AND SKILL (TKS) STATEMENT REVIEW UPDATE

Dylan provided a general overview of the development of the TKS Statements review and process provided by of Project Team 1: Risk Assessment (ID.RA-P) and Project Team 2: Inventory and Mapping (ID.IM-P).

Currently, the PWWG Co-Chairs have completed Round 3 of their review of the TKS Statements, and their comments and recommendations will be provided to the Project Team Leads by the end of the week. In addition, they are also reviewing the baseline TKS Statements aligned with the Privacy Framework Core, the IDENTIFY-P (ID-P) Function, and the Inventory and Mapping Category as submitted by Project Team 2. The PWWG Co-Chairs will review and discuss how to utilize the baseline TKS Statements to either be provided as 1) information for future Project Teams, 2) a standalone document, and/or 3) a reference material resource.

Dylan also noted that the PWWG will await work on the PROTECT-P Function (PR-P) until after the NIST National Initiative for Cybersecurity Education Program completes their updates to their TKS Statements that will eventually map to PR-P.

The next PWWG Co-Chairs review is planned for January 2022. In addition, Dylan provided an overview of the TKS Statement review and submission process.

- 1) The Project Teams work on their TKS Statements for their specified Subcategories.
- 2) Simultaneously, the Project Team Leads may provide a subset of their completed TKS Statements to the PWWG Co-Chairs for review.
- 3) After the initial PWWG Co-Chair review, the Project Team Leads review feedback and recommendations, in addition to discussions with the Project Team members to agree with the Co-Chair recommendations, provide additional feedback, or to provide additional modifications to their submitted TKS Statements.
 - a. Recommendations provided by the PWWG Co-Chairs is guidance and not necessarily mandated.
- 4) After, the Co-Chair have agreed to the TKS Statements submitted, they are considered final and completed.
- 5) The entire PWWG will be provided with an opportunity to review the final TKS Statements and provide comments and/or feedback.

C. IAPP PRIVACY SECURITY RISK CONFERENCE – ROUNDTABLE REPORT

During the International Association of Privacy Professionals (IAPP) Conference in October 2021, the NIST hosted a public roundtable session, “Growing a Workforce for Managing Privacy Risk.” The goal of the roundtable session was to discuss amongst stakeholder’s privacy workforce challenges, useful tools and resources, desired skill and knowledge sets, workforce recruitment and development, and ownership and responsibilities.

The stakeholders discussed other areas of concern in relation to privacy workforce:

- 1) Resource constraints – e.g., money, people – and reliance on vendors.
- 2) Challenges moving from legal to operations while identifying internal compliance and the need for clear individual and/or shared roles and responsibilities.
- 3) Collaboration and communication amongst internal and external stakeholders at various levels.

- 4) Desire for both flexible and notional PWWG resources. For example, benefiting from higher level Task, Knowledge, and Skill (TKS) Statements for hiring activities.
- 5) Training material is critical.
- 6) Recruiting (HR) resources are helpful and different from training material.

III. PROJECT TEAM UPDATES

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

Dylan advised that the Project Team Co-Leads, Lauren Jones, Privacy Counsel, Surescripts, LLC, and Lisa McKee Senior Manager Security and Data Privacy, Protiviti, were not present during this call. Dylan provided a brief background and status update of the Project Team 1: Risk Assessment (ID.RA-P) Task, Knowledge, and Skill (TKS) Statements.

For reference purposes, the Team is tasked with the development of the TKS Statements for five (5) Subcategories from the NIST Privacy Framework Core V1¹.

IDENTIFY-P (ID-P): Develop the organizational understanding to manage privacy risk for individuals arising from data processing.

- **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.
 - **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.

Dylan noted that Project Team 1 has completed and submitted their TKS Statements to the PWWG Co-Chairs for Subcategory ID.RA-P1. Upon receipt of the PWWG Co-Chairs recommendations, the Team will review and provide their comments and/or revisions back to the PWWG Co-Chairs during January 2022.

Currently, the Project Team has completed their initial review of Subcategory ID.RA-P2 and will submit their TKS Statements to the Co-Chairs for review. The Project Team will continue to discuss and finalize their TKS Statements for Subcategories ID.RA-P3, ID.RA-P4, and ID.RA-P5. Subcategory ID.RA-P3 will be discussed during their upcoming meetings in January 2022. The Project Team estimates their completion of the TKS Statements by March 2022.

Dylan encouraged NIST PWWG members who are interested in providing further information on this topic, to join the NIST PWWG Project Team 1 Mailing List, please see the Join Mailing List

¹ [NIST Privacy Framework Core](#)

section under Section V. Next Steps and Upcoming Meetings.

B. UPDATE OF PROJECT TEAM 2: INVENTORY AND MAPPING (ID.IM-P) ACTIVITIES

Project Team Co-Lead, Dr. Sarah Lewis Cortes, Privacy Engineering, Netflix, and Mary Potter, Director of Privacy and Research Data Protections, Virginia Tech, provided a brief background and status of Project Team 2: Inventory and Mapping (ID.IM-P) Task, Knowledge, and Skill (TKS) Statements.

For reference purposes, the team is tasked with the development of the Task, Knowledge, and Skill (TKS) Statements for eight (8) Subcategories from the NIST Privacy Framework Core V1².

- **IDENTIFY-P (ID-P):** Develop the organizational understanding to manage privacy risk for individuals arising from data processing.
 - **Inventory and Mapping (ID.IM-P):** Data processing by systems, products, or services is understood and informs the management of privacy risk.
 - **ID.IM-P1:** Systems/products/services that process data are inventoried.
 - **ID.IM-P2:** Owners or operators (e.g., the organization or third parties such as service providers, partners, customers, and developers) and their roles with respect to the systems/products/services and components (e.g., internal, or external) that process data are inventoried.
 - **ID.IM-P3:** Categories of individuals (e.g., customers, employees or prospective employees, consumers) whose data are being processed are inventoried.
 - **ID.IM-P4:** Data actions of the systems/products/services are inventoried.
 - **ID.IM-P5:** The purposes for the data actions are inventoried.
 - **ID.IM-P6:** Data elements within the data actions are inventoried.
 - **ID.IM-P7:** The data processing environment is identified (e.g., geographic location, internal, cloud, third parties).
 - **ID.IM-P8:** Data processing is mapped, illustrating the data actions and associated data elements for systems/products/services, including components; roles of the component owners/operators; and interactions of individuals or third parties with the systems/products/services.

Project Team Co-Lead, Mary Potter, discussed an overview of the Teams activities for November 2021. The Project Team completed and submitted all Subcategories for Inventory and Mapping (ID.IM-P1 through ID.IM-P8) to the PWWG Co-Chairs for review. The Project Team is currently reviewing and discussing the feedback from the Co-Chairs for ID.IM-P1 through ID.IM-P6. In addition, the Project Team also submitted their suggestions for overall baseline TKS Statements for the NIST Privacy Framework, the Identify-P Function, and the Inventory and Mapping (ID.IM-P) Category.

Project Team Co-Lead, Sarah Cortes, discussed various topics of interest that the Project Team members had discussed and debated. Such as whether “all systems, processes, services” should be general tasks or only those specific to privacy impact.

Additional topics included the maintenance of Tasks in relation to the CMMI (Capability Maturity

² [NIST Privacy Framework Core](#)

Model Integration) Model suggesting that the assumption would be that all Tasks must be maintained and continuously updated over time. However, the Project Team would like to discuss further and receive feedback for a consensus on how to address this topic throughout the Privacy Framework's Tasks, Knowledge, and Skill (TKS) Statements.

Project Team Co-Lead, Sarah Cortes, also discussed the use of examples, although some Subcategories already include examples. It was noted that the inclusion of examples is generally helpful to the end user although they are not comprehensive and is subject to a company's operations.

Classification of identifiers was noted as the last topic of discussion. Although identifiers are more specific to the Inventory and Mapping Category there may be more areas within the Privacy Framework where classifying identifiers may be relevant. In addition to data element identifiers being classified by identifier types.

The Project Team Co-Lead, Sarah Cortes discussed the challenges and lessons learned within the Project Team throughout their development of TKS Statements. Some of the areas discussed in reference to the development of TKS Statements, were the timeframe, and having a more iterative process with the PWWG Co-Chairs initially to ensure that the Project Teams are on track.

The Project Team will continue to discuss and refine their current TKS Statements in coordination with the PWWG Co-Chairs review and feedback to present final TKS Statements. The PT2 Meeting scheduled for December 27, 2021 will be cancelled and the team will resume on Monday, January 10, 2021 at 12:00 P.M EST.

The Project Team Co-Leads encouraged the expertise and perspectives of the NIST PWWG Membership to participate in the review process of the TKS Statements.

IV. Q & A

N/A

V. NEXT STEPS & UPCOMING MEETINGS

A. NEXT STEPS

- Project Teams will continue to review, refine, and finalize TKS Statements and submit to the Co-Chairs for review and comment.
- Co-Chairs will continue to review initial TKS Statements and will provide feedback to the Project Teams to discuss and provide a consensus.
- NIST will start to commence Project Team 3: Policies, Processes, and Procedures.
- The Co-Chairs will select the Project Team 3 Co-Leads and provide an announcement during the January PWWG Monthly meeting.
- 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 and updated meeting schedules, please visit the [PWWG web page](#).

1) Project Team 1: Risk Assessment (ID.RA-P)

- Wednesday, December 15, 2021 | 5:00PM – 6:00PM ET
- Thursday, January 6, 2021 — 11:00am ET – 12:00pm ET

2) Project Team 2: Inventory and Mapping (ID.IM-P)

- Monday, December 13, 2021 — 12:00pm ET – 1:00pm ET
- Monday, January 10, 2021 — 12:00pm ET – 1:00pm ET
 - The meeting scheduled for Monday, December 27, 2021 is cancelled.

3) NIST Privacy Workforce Public Working Group

The NIST PWWG Monthly Meeting is the 2nd Wednesday of each month. Meeting dates, minutes, and slides are located on the PWWG website.

- Wednesday, January 12, 2021 — 1:00pm ET – 2:00pm ET

C. JOIN MAILING LIST:

- E-mail addresses for members to join/subscribe:
 - Privacy Workforce Working Group (PWWG):
PrivacyWorkforceWG+subscribe@list.nist.gov
 - Project Team 1 (PT1): PrivacyWorkforcePT1+subscribe@list.nist.gov
 - Project Team 2 (PT2): PrivacyWorkforcePT2+subscribe@list.nist.gov
- Please be reminded to review adhere to the Mailing List Rules that can be accessed on the [NIST PWWG web page](#).

D. TROUBLESHOOTING:

If you should have issues with meeting invitations, mailing lists, and/or accessing the Google Drives, please email NIST PWWG Support at PWWG@nist.gov