

NIST PRIVACY WORKFORCE PUBLIC WORKING GROUP (PWWG)

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

MEETING MINUTES

Wednesday, June 8, 2022

1:00 P.M. ET – 2:00 P.M. ET

I. INTRODUCTION

The 14th meeting of the National Institute of Standards and Technology (NIST) Privacy Workforce Public Working Group (PWWG) convened on Wednesday, June 8, 2022, 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 introduction of the Co-Leads for Project Team 3 and Project Team 5, PWWG Co-Chair Review of Task, Knowledge, and Skill (TKS) Statements, and Project Team updates from Project Team 1: Risk Assessment (ID.RA-P), Project), and Project Team 3: Policies, Processes, And Procedures (GV.PO-P, CT.PO-P, and CM.PO-P), and Project Team 4 (Data Ecosystem).

II. PWWG UPDATES

Co-Chair: Dylan Gilbert provided a brief update of the general status of the current and new PWWG Project Teams.

A. NIST PRIVACY FRAMEWORK AND PWWG TKS MAPPING

The completed TKS Statements are mapped to the Privacy Framework Core Categories and Subcategories. The PWWG membership will have read-only access to this TKS Reference Document via the shared Google Drive¹ to view the final TKS Statements submitted by Project Teams. The TKS Reference Documents are noted below:

- PWWG TKS Statements Final (version 1) Inventory²
- PWWG TKS Statements Final (version 1) Subcategories³

Project Team 1 (Risk Assessment) is nearing completion and will be the next Category to be added to the TKS Reference Documents. The PWWG membership will have an opportunity to provide comments and feedback on the final TKS Statements within the near future.

B. RESOURCES DISCUSSION

Upon completion of PWWG TKS Statements, the group will reassess whether to initiate a second phase of resource creation. Although, the PWWG membership agreed that Resources (e.g., explanatory notes, citations, etc.) would be helpful, at this time, the PWWG will continue to focus on the development of TKS Statements. Upon completion of PWWG TKS Statements, the PWWG membership may initiate a second phase to create a comprehensive approach and methodology

¹ [PWWG Reference Documents - Google Drive](#)

² [PWWG | PWWG TKS Statements Final \(version 1\) Inv](#)

³ [PWWG TKS Statements Final \(version 1\) Sub](#)

for the development and maintenance of the supplemental resources.

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

The PWWG Co-Chairs have selected an additional Project Team 3 Co-Lead to replace Amin Ali. Alicia Christensen has joined Project Team 3 as an additional Co-Lead to assist Dan LoPresto and Nandita Narla in the development of TKS Statements. Alicia Christensen was present and provided a brief background of her relevant experience to the PWWG Membership.

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

The PWWG Co-Chairs have selected the Project Team 5 Co-Leads and Dylan provided a brief welcome and introduction. Anshu Gupta was present and provided a brief background of his relevant to the PWWG membership. Brandi Bennett was not present; however, Dylan provided a brief introduction in Brandi's absence. It was also noted that Project Team 5 will be developing TKS Statements for the final Category (Business Environment) to be completed within the Identify (ID-P) function of the Privacy Framework.

III. PROJECT TEAM UPDATES

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

PWWG Co-Chair, Dylan Gilbert, provided a brief background and status update of the Project Team 1: Risk Assessment (ID.RA-P) TKS Statements. Project Team Co-Leads Lauren Jones, Privacy Counsel, Surescripts, LLC and Lisa McKee, Director of Governance, Risk, Compliance and Privacy, Hudl were not present during this call.

For reference purposes, Project Team 1 is tasked with the development of the TKS Statements for five (5) Subcategories from the NIST Privacy Framework Core V1⁴.

IDENTIFY-P (ID-P): Develop the organizational understanding to manage privacy risk for individuals a rising 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 discrepancies remain between some of the Team's proposed TKS Statements

⁴ [NIST Privacy Framework Core](#)

and the Co-Chairs recommended revisions. The Team will continue to discuss and finalize their TKS Statements for Subcategory ID.RA-P1, ID.RA-P3, ID.RA-P4, and ID.RA-P5. The Team has previously agreed to have (2) additional meetings at the (1) at the end of May and (1) at the end of June 2022 to assist with completing the review from the PWWG Co-Chairs.

In addition, ID.RA-P2 is still in the process of review and discussion between the NIST Privacy Engineering Program and Artificial Intelligence Teams.

In the month of June 2022, the team will continue to address and finalize their TKS Statements in response to the PWWG Co-Chairs feedback and comments. The Project Team estimates their completion of the TKS Statements by end of July 2022.

The Project Team is no longer accepting new members and encouraged the expertise and perspectives of the NIST PWWG membership to participate in the new Project Teams 3, 4, and 5. To join the NIST PWWG Project Team 3, Project Team 4, or Project Team 5 Mailing List, please see the Join Mailing List Section under Section V. Next Steps and Upcoming Meetings.

B. UPDATE OF PROJECT TEAM 3: POLICIES, PROCESSES, AND PROCEDURES ACTIVITIES

Project Team Co-Leads, Dan LoPresto, Director of Privacy Compliance, University of Central Florida, and Nandita Narla, Senior Privacy Program Manager for Privacy, welcomed and thanked the new Project Team Co-Lead Alicia Christensen, VP, General Counsel, Chief Compliance Officer at National Jewish Health Principal Advisor, Frame Privacy Group, who will replace the previous Project Team Co-Lead Amin Ali. Dan LoPresto provided a brief background and status of Project Team 3: Policies, Processes, and Procedures (GV.PO-P, CT.PO-P, and CM.PO-P) TKS Statements and activities.

For reference purposes, the NIST PWWG Project Team 3: Policies, Processes, and Procedures, will create TKS Statements for (12) Subcategories from the NIST Privacy Framework Core V1.

- **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.

Project Team Co-Lead: Dan LoPresto provided a brief update of Project Team 3 activities. The Project Team has currently started to develop draft TKS Statements for GV.PO-P5 and plans to finish the 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.”) Category within the month of June 2022.

The Project Team will continue brainstorm and develop TKS Statements for GV.PO-P5 and GV.PO-P6 during their next meeting. The Team plans to submit their proposed TKS Statements to the PWWG Co-Chairs for GV.PO-P1 through P4 in June 2022.

The Project Team Co-Leads encourage the expertise and perspectives of the NIST PWWG Membership to participate in the development process of the TKS Statements. To join the NIST PWWG Project Team 3 Mailing List, please see the Join Mailing List Section under Section V. Next Steps and Upcoming Meetings.

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

Project Team Co-Leads, Tahir Latif, Head of Practice - Data Protection, Artificial Intelligence and Analytics (APAC & EMEA) Cognizant Worldwide, Paul Lanois, Director, Fieldfisher, and Anne Connell Senior Cybersecurity Engineer, Carnegie Mellon University, were present and provided a brief update.

For reference purposes, the NIST PWWG Project Team 4: Data Processing Ecosystem, will create TKS Statements for (5) Subcategories from the NIST Privacy Framework Core V1.

CATEGORY: 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:

- 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 Co-Lead Tahir Latif provided a brief update of Project Team 4 activities. The Project Team has completed the TKS Statements for ID.DE-P1 and is currently working on 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.). In addition to ensuring that there is uniformity and the proposed TKS Statements are in alignment with the Authoring Guide⁵.

The Project Team Co-Lead, Tahir Latif also discussed the challenges and lessons learned within the

⁵ [Task Knowledge Skill \(TKS\) Statements Authoring Guide for Workforce Frameworks](#)

Project Team throughout their development of TKS Statements. Some of the areas discussed in reference to the development of TKS Statements, were as follows:

- Ensuring that the Project Team members are currently on track.
- Acknowledging and ensuring that the new Project Team members understand the mission, goals, and current working status of the Project Team.
- Keeping the focus of discussions within a specific subcategory.
- Productive use of meeting time.

It was reiterated that the Project Team Co-Leads would encourage the Project Team members to continue to provide their proposed TKS Statements and comments in between meetings in preparation for discussion.

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

The Project Team 4 Mailing List is currently open for those interested in participating. To join the NIST PWWG Project Team 4 Mailing List, please see the Join Mailing List Section under Section V. Next Steps and Upcoming Meetings.

IV. Q & A

Question: How many Project Teams remain within the PWWG?

Answer: There are (18) Categories in total for the Privacy Framework:

- (2) Categories are complete (ID.IM-P, ID.RA-P)
- (5) Categories are active (GV.PO-P, CM.PO-P, CT.PO-P, ID.BE-P, ID.DE-P)
- (5) Categories in the Protect Function that will be addressed and mapped to the NICE Framework. The NICE team is currently updating their TKS Statements, and many will overlap with the Cybersecurity Framework and the Privacy Framework.
- (6) Categories remaining in the areas of Govern, Control, and Communicate.

Therefore, we will have a maximum of (6) Project Team remaining. However, it may change due to combining multiple Categories to be addressed within (1) Project Team similar to Project Team 3. This will be determined on an as needed basis in the near future.

Question: When is this effort slated to complete for entire Privacy Framework?

Answer: Completion of the Categories within the Privacy Framework is estimated to be as soon as possible, the pace and rate of progress within the Project Teams has picked up abundantly.

Question: Within the Data Ecosystem, are we developing specific TKS Statements for the various tiers (i.e., public, private, and government)?

Answer: The TKS Statements are broadly applicable and law, technology, and sector agnostic. At this time, we have not differentiated between public/ non-public organizations, technical, business operational, and management types in relation to the data processing ecosystem. However, communities of interest could be created to generate sector-specific content once the PWWG has completed its initial work. It is encouraged that

interested PWWG members join the Project Teams.

V. NEXT STEPS & UPCOMING MEETINGS

• NEXT STEPS

- Project Team 1: Risk Assessment (ID.RA-P) will continue to address the recommendation from the PWWG Co-Chairs to finalize their TKS Statements.
- Project Team 3: Policies, Processes, and Procedures (GV.PO-P, CM.PO-P, CT.PO-P) will continue to discuss and develop TKS Statements.
- Project Team 4: Data Processing Ecosystem Risk Management (ID.DE-P) will continue to discuss and develop TKS Statements.
- Project Team 5: Business Environment (ID.BE-P) is estimated to start mid/end of July 2022.

• 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 [NIST Privacy Workforce Working Group](#) website.

- **Project Team 1: Risk Assessment (ID.RA-P)**
 - Wednesday, June 15, 2022 | 5:00pm - 6:00pm ET
- **Project Team 3: Policies, Processes, and Procedures (GV.PO-P, CM.PO-P, CT.PO-P)**
 - Thursday, June 9, 2022 | 1:00pm ET – 2:00pm ET
- **Project Team 4: Data Processing Ecosystem Risk Management (ID.DE-P)**
 - Thursday, June 16, 2022 | 2:00pm ET – 3:00pm ET
- **NIST Privacy Workforce Public Working Group**
 - Wednesday, July 13, 2022 | 1:00pm ET – 2:00pm ET

• 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.

• JOIN MAILING LIST

All mailing lists are moderated. Please be reminded to review adhere to the Mailing List Rules that can be accessed on the [NIST Privacy Workforce Working Group](#) website.

- E-mail addresses for members to join/subscribe:
 - Privacy Workforce Working Group (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

• 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