

# NIST PRIVACY WORKFORCE PUBLIC WORKING GROUP (PWWG)

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

## MEETING MINUTES

Wednesday, March 9, 2022

1:00 P.M. ET – 2:00 P.M. ET

### I. INTRODUCTION

The (11<sup>th</sup>) meeting of the National Institute of Standards and Technology (NIST) Privacy Workforce Public Working Group (PWWG) convened on Wednesday, March 9, 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 NIST PWWG Project Team 4, 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 Team 2: Inventory and Mapping (ID.IM-P), and Project Team 3: Policies, Processes, And Procedures (GV.PO-P, CT.PO-P, and CM.PO-P).

### 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 PWWG PROJECT TEAM 2: INVENTORY AND MAPPING (ID.IM-P)

Project Team 2 is currently wrapping up a few details regarding their TKS Statements. Dylan thanked and congratulated the Project 2 Team Co-Leads and their members for their completed TKS Statements. It was also noted that the PWWG membership will have an opportunity to provide feedback on completed TKS Statements in the future.

It was stated that at any given time, there will be (3) Project Teams operating within the PWWG. Therefore, since Project Team 2 has completed their work, the launch of Project Team 4 has started.

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

Project Team 3 has started to develop TKS Statements for their (3) Categories and its Subcategories.

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

Project Team 4 has launched and will have their first meeting on Thursday, March 10, 2022, at 3:00pm ET. The Co-Leads will be announced and will provide a brief introduction after the Project Team updates.

#### D. NIST PRIVACY FRAMEWORK AND PWWG TKS MAPPING

The NIST Team is currently developing a strategy to document and map completed TKS Statements to Privacy Framework Core Categories and Subcategories. The PWWG membership will have read-only access to this TKS Reference Document via the shared Google Drive to view

the final TKS Statements submitted by Project Teams. The NIST Team is targeting the end of March 2022 to make this information available. When the Project Teams wind down, the PWWG membership will have an opportunity to provide comments and feedback on the final TKS Statements.

#### **E. PWWG CO-CHAIRS TKS STATEMENT REVIEW UPDATE**

Dylan provided a general overview of the development of the TKS Statements review process. Currently, the PWWG Co-Chairs are reviewing Project Team 1 TKS Statements for ID.RA-P1, ID.RA-P2, ID.RA-P3, and ID.RA-P4. The next PWWG Co-Chairs review is planned for March 24, 2022.

In addition, it was also noted that the NIST PWWG Team implemented a new policy of open invitation for Project Team Co-Leads to participate in the review sessions.

### **III. PROJECT TEAM UPDATES**

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

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

For reference purposes, the Team is tasked with the development of the TKS Statements for five (5) Subcategories from the NIST Privacy Framework Core V1<sup>1</sup>.

**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.

Project Team Co-Lead Lisa McKee noted that Project Team 1 has completed their TKS Statements for ID.RA-P1, ID.RA-P2, ID.RA-P3, and ID.RA-P4. Currently, the Project Team will continue to discuss and finalize their TKS Statements for Subcategory ID.RA-P5 to submit for review by the PWWG Co-Chairs. The Project Team estimates their completion of the TKS Statements by end of March 2022.

---

<sup>1</sup> [NIST Privacy Framework Core](#)

In the month of April 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 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 and 4. To join the NIST PWWG Project Team 3 or Project Team 4 Mailing List, please see the Join Mailing List 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, 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) TKS Statements. Project Team Co-Lead, Dr. Sarah Lewis Cortes, Privacy Engineering, Netflix, was not present during this call.

For reference purposes, the team is tasked with the development of the TKS Statements for eight (8) Subcategories from the NIST Privacy Framework Core V1.

- **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 February 2022. The Project Team completed, revised, and resubmitted all Subcategories for Inventory and Mapping (ID.IM-P1 through ID.IM-P8) to the PWWG Co-Chairs for finalization. The Project Team incorporated changes and updates received from the PWWG Co-Chairs and the team members.

Project Team Co-Lead, Mary Potter provided acknowledgements and thank you's to the Project Team members, the PWWG Co-Chairs, and the NIST PWWG Team for their contributions and guidance.

Although, Project Team 2 has concluded their meetings. The Project Team Co-Leads are currently refining the last few TKS Statements and will distribute a survey indicating the suggested associations, changes, and/or comments, to the team members for review.

A survey will be circulated to the Project Team members to review and agree by consensus on a few TKS Statements for finalization. The survey is estimated to be distributed during the week of March 14, 2022.

Completed TKS Statements from Project Team 2 will be included in the Reference Document.

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 and 4. To join the NIST PWWG Project Team 3 or Project Team 4 Mailing List, please see the Join Mailing List Section under Section V. Next Steps and Upcoming Meetings.

#### **C. UPDATE OF PROJECT TEAM 3: POLICIES, PROCESSES, AND PROCEDURES ACTIVITIES**

Project Team Co-Leads, Amin Ali, GRC Program Manager & Cybersecurity PMO Lead, Motorola Solutions, Dan LoPresto, Director of Privacy Compliance, University of Central Florida, and Nandita Narla, Senior Privacy Program Manager for Privacy, 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.

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-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.).

The Project Team will continue brainstorm and development TKS Statements during their next meeting.

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.

- D. 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, provided brief individual introductions as the Project Team Co-Leads Project Team 4: Data Processing Ecosystem Risk Management (ID.DE-P).

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.

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.

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**

N/A

## V. NEXT STEPS & UPCOMING MEETINGS

### A. NEXT STEPS

- Project Team 1 will continue to work with the PWWG Co-Chairs to finalize their TKS Statements.
- Project Team 3 will continue to discuss and develop TKS Statements.
- Project Team 4: Data Processing Ecosystem Risk Management (ID.DE-P) will hold their first meeting.
- NIST will continue to develop the Privacy Framework and PWWG TKS Statement Mapping.

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

- **Project Team 1: Risk Assessment (ID.RA-P)**
  - Wednesday, March 16, 2022 | 5:00pm - 6:00pm ET
- **Project Team 2: Inventory and Mapping (ID.IM-P)**
  - Completed
- **Project Team 3: Policies, Processes, and Procedures (GV.PO-P, CM.PO-P, CT.PO-P)**
  - Thursday, March 17, 2022 | 1:00pm ET – 2:00pm ET
- **Project Team 4: Data Processing Ecosystem Risk Management (ID.DE-P)**
  - Thursday, March 10, 2022 | 3:00pm ET – 4:00pm ET
- **NIST Privacy Workforce Public Working Group**
  - Wednesday, April 13, 2022 | 1:00pm ET – 2:00pm 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. 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](mailto:PrivacyWorkforceWG+subscribe@list.nist.gov)
  - Project Team 3 (PT3): [PrivacyWorkforcePT3+subscribe@list.nist.gov](mailto:PrivacyWorkforcePT3+subscribe@list.nist.gov)
  - Project Team 4 (PT4): [PrivacyWorkforcePT4+subscribe@list.nist.gov](mailto:PrivacyWorkforcePT4+subscribe@list.nist.gov)

### E. 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](mailto:PWWG@nist.gov)