

NIST PRIVACY WORKFORCE PUBLIC WORKING GROUP (PWWG)

Co-Chair: Dylan Gilbert, NIST Privacy Policy Advisor

MONTHLY MEETING MINUTES Wednesday, December 13, 2023 1:00 P.M. ET – 2:00 P.M. ET

I. INTRODUCTION

The 30th meeting of the National Institute of Standards and Technology (NIST) Privacy Workforce Public Working Group (PWWG) convened on Wednesday, December 13th from 1:00 P.M. - 2:00 P.M. ET virtually via Microsoft Teams. There were 27 attendees.

The PWWG provides a forum for participants from the 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](#) and the National Initiative for Cybersecurity Education (NICE) [Workforce Framework for Cybersecurity](#).

PWWG Co-Chair, Dylan Gilbert, welcomed attendees to the meeting. He noted that the meeting would be shorter than usual, but he wanted to announce the status of the newest and final Project Teams.

II. PWWG UPDATE

A. PROJECT TEAM LEAD APPRECIATION

Project Team 7 has completed its work on drafting TKS Statements for the Awareness and Training Category in the Govern Function. Dylan thanked the Co-Leads of PT7, Jacqueline Crawley, Ivy Orecchio, and Elif Kiesow Cortez for their efforts in leading the Project Team and completing work on the four Subcategories. He also thanked the members who participated in the meetings and shared their expertise.

B. PWWG TIMELINE UPDATE

Dylan discussed the timeline for completion of the TKS Statements and the revised schedule for the launch of the final Project Teams. The current and new Project Teams will be on a very tight schedule. The NIST Privacy team goal is to get the initial Privacy Workforce Taxonomy Public Draft out in April, 2024. There will be a public comment period and then Version 1.0 of the Privacy Workforce Taxonomy will be published targeting the summer of 2024.

The final Project Teams, PT9, PT10, and PT11 will be working on the remaining Subcategories which will run from December through March, 2024. The teams may need to work on a weekly basis instead of the biweekly cadence of the previous teams.

PT9 Data Processing Awareness (CM.AW-P) - 8 Subcategories

PT10 Monitoring and Review (GV.MT-P) - 7 Subcategories

PT11 Disassociated Processing (CT.DP-P) - 5 Subcategories

Project Team 9 has already begun its biweekly meetings. Project Team 10 and Project Team 11 Co-Leads have started the prework and will begin team meetings in early January. This gives them 10 weeks to go through the remaining 12 Subcategories.

Dylan reminded all Project Team members that the intent is for work to happen outside of team meetings. All members are encouraged to review and submit comments in the Google Workbooks between meetings so that the teams can discuss these ideas during the scheduled meetings. That work will be even more important with the new compressed schedule. The PWWG is sprinting to the finish line!

C. NEW PROJECT TEAMS PT10 AND PT11

Dylan announced that the Co-Leads for the two newest Project Teams have been selected. He noted that it was good to have Sarah Cortes back to serve again as a Co-Lead. Sarah previously served as a Co-Lead for Project Team 2 (Inventory and Mapping).

Project Team 10 - Monitoring and Review (GV.MT-P) – 7 Subcategories

- Co-Leads: Catherine Tomasi, Director and CPO, Con Edison
- Robert Taboada, Privacy Specialist, Amazon
- Phil Lowry, Senior Counsel, Remitly

Project Team 11: Disassociated Processing (CT.DP-P) – 5 Subcategories

- Sarah Lewis Cortes, Privacy Engineer, Netflix
- Hank Roser, Privacy Engineer, Consumer Financial Protection Board
- Sri Maddipati, Senior Privacy Engineer, Google

Robert Taboada, Amazon, and Hank Roser, CFPB introduced themselves to the attendees.

Project Teams 10 and 11 will hold their kickoff meetings in early January. The Project Team Google Groups are already open for those who wish to join. See the links to join these teams in the Mailing List section below.

III. PROJECT TEAM UPDATES

A. UPDATE OF PROJECT TEAM 6: RISK MANAGEMENT STRATEGY

GOVERN-P (GV-P): Develop and implement the organizational governance structure to enable an ongoing understanding of the organization's risk management priorities that are informed by privacy risk.

- **Risk Management Strategy (GV.RM-P):** The organization's priorities, constraints, risk tolerances, and assumptions are established and used to support operational risk decisions.
 - **GV.RM-P1:** Risk management processes are established, managed, and agreed to by organizational stakeholders.
 - **GV.RM-P2:** Organizational risk tolerance is determined and clearly expressed.
 - **GV.RM-P3:** The organization's determination of risk tolerance is informed by its role(s) in the data processing ecosystem.

Dylan gave the team update for Project Team 6. Dylan noted the great work that PT6 has done with the Risk Management Strategy Category. The work is almost complete. The Co-Chairs will complete their review of the remaining Subcategory (GV.RM-P3) this week. It is possible that there may be one more ad hoc meeting for PT6 but most likely the Co-Leads can finish it without a meeting. Dylan thanked the members of PT6 for all of their work on this foundational Category.

B. UPDATE OF PROJECT TEAM 8: DATA PROCESSING MANAGEMENT (CT.DM-P)

CONTROL-P (CT-P): Develop and implement appropriate activities to enable organizations or individuals to manage data with sufficient granularity to manage privacy risks.

- **Data Processing Management (CT.DM-P):** Data are managed consistent with the organization's risk strategy to protect individuals' privacy, increase manageability, and enable the implementation of privacy principles (e.g., individual participation, data quality, data minimization).
 - **CT.DM-P1:** Data elements can be accessed for review.

- **CT.DM-P2:** Data elements can be accessed for transmission or disclosure.
- **CT.DM-P3:** Data elements can be accessed for alteration.
- **CT.DM-P4:** Data elements can be accessed for deletion.
- **CT.DM-P5:** Data are destroyed according to policy.
- **CT.DM-P6:** Data are transmitted using standardized formats.
- **CT.DM-P7:** Mechanisms for transmitting processing permissions and related data values with data elements are established and in place.
- **CT.DM-P8:** Audit/log records are determined, documented, implemented, and reviewed in accordance with policy and incorporating the principle of data minimization.
- **CT.DM-P9:** Technical measures implemented to manage data processing are tested and assessed.
- **CT.DM-P10:** Stakeholder privacy preferences are included in algorithmic design objectives and outputs are evaluated against these preferences.

Project Team 8 (PT8) Co-Lead, Nikita Samarin, provided the update. PT8 is close to completing its work with only two Subcategories remaining. Nikita expects that the team will finish its work on December 21. Nikita noted that the team has made a lot of progress this month since they switched to a weekly meeting schedule. They have had a consistent group of attendees which has been very helpful.

Nikita noted the challenge of making sure that their TKS Statements could work for an organization that was just starting out, not just for mature organizations.

Dylan noted that PT8 had a big lift with ten Subcategories. The first four were similar which helped with leveraging work done on the first in the others. There was a lot of discussion about how granular or high level to make the TKS Statements, and making sure that everyone was on the same page with terminology.

Nikita invited anyone who is interested to join the team to help work on the final Subcategories.

C. UPDATE OF PROJECT TEAM 9: DATA PROCESSING AWARENESS (CM.AW-P)

COMMUNICATE-P (CM-P): Develop and implement appropriate activities to enable organizations or individuals to manage data with sufficient granularity to manage privacy risks.

- **Data Processing Awareness (CM.AW-P):** Individuals and organizations have reliable knowledge about data processing practices and associated privacy risks, and effective mechanisms are used and maintained to increase predictability consistent with the organization's risk strategy to protect individuals' privacy.
 - **CM.AW-P1:** Mechanisms (e.g., notices, internal or public reports) for communicating data processing purposes, practices, associated privacy risks, and options for enabling individuals' data processing preferences and requests are established and in place.
 - **CM.AW-P2:** Mechanisms for obtaining feedback from individuals (e.g., surveys or focus groups) about data processing and associated privacy risks are established and in place.
 - **CM.AW-P3:** System/product/service design enables data processing visibility.
 - **CM.AW-P4:** Records of data disclosures and sharing are maintained and can be accessed for review or transmission/disclosure.
 - **CM.AW-P5:** Data corrections or deletions can be communicated to individuals or organizations (e.g., data sources) in the data processing ecosystem.
 - **CM.AW-P6:** Data provenance and lineage are maintained and can be accessed for review or transmission/disclosure.
 - **CM.AW-P7:** Impacted individuals and organizations are notified about a privacy breach or event.

- **CM.AW-P8:** Individuals are provided with mitigation mechanisms (e.g., credit monitoring, consent withdrawal, data alteration or deletion) to address impacts of problematic data actions.

New PT9 Co-Leads Paul Lanois and Shoshana Rosenberg gave the team update. Paul noted that the team has held two meetings and they are now working on the second Subcategory. The next PT9 meeting is tomorrow, and they will break for the holidays and pick back up in January.

Shoshana pointed out that having the baseline TKS Statements in the TKS Workbook has been very useful to the team. The Co-Leads welcome anyone who is interested to join them on the team.

IV. Q & A

Question: Is there a Crosswalk between the NIST Cybersecurity Framework (CSF) and the NICE Framework?

Answer: Dylan noted that he was not aware of a crosswalk between the CSF and the NICE Framework. The NICE team is currently in the process of updating their TKS Statements. The CSF also is in a state of change with the release of the CSF 2.0 initial public draft in August 2023.

Dylan assured everyone that the intent of the Privacy team is to map the PWWG TKS Statements to the Privacy Framework.

There are still open questions regarding the CSF 2.0 update and the potential issues of realigning the Privacy Framework to CSF 2.0. The new CSF 2.0 has what they are calling implementation examples. The NIST Privacy team is in meetings with the CSF team to discuss whether those are going to include, for example, TKS statements from the NICE Framework or maybe even some from the PWWG Taxonomy.

Once the NICE Framework team has completed their updates, the intent is for the PWWG to be able to leverage some of their TKS Statements in the Protect Function. Dylan invited anyone who feels inspired to do so, to submit any suggestions they may have for the Protect Function to the PWWG team. The NIST Team is open to looking at anything that is submitted.

Once the Privacy Workforce Taxonomy is complete it will be put out for a public comment period, and everyone will have a chance to weigh in.

Dylan suggested that he may invite the NICE team to join the PWWG meeting in January or February to give an update on the progress they are making with the NICE Framework.

V. NEXT STEPS & UPCOMING MEETINGS

A. 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 7 (PT7)

- Next Meeting: As needed – TBD.

Project Team 8 (PT8)

- Next Meeting: Thursday, December 14, 2023 | 11:00am – 12:00pm ET

Project Team 9 (PT9)

- Meeting: Thursday, December 14, 2023 | 2:00pm – 3:00pm ET

Project Team 10 (PT10)

- Meeting: TBD – January 2024

Project Team 11 (PT11)

- Meeting: TBD – January 2024

NIST Privacy Workforce Public Working Group

- Wednesday, October 8, 2023 | 1:00pm – 2:00pm ET

B. 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.

C. 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.

D. JOIN MAILING LIST

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
- PT8 (CT.DM-P): PrivacyWorkforcePT8+subscribe@list.nist.gov
- PT9 (CM.AW-P): PrivacyWorkforcePT9+subscribe@list.nist.gov
- PT10 (GV.MT-P): PrivacyWorkforcePT10+subscribe@list.nist.gov
- PT11 (CT.DP-P): PrivacyWorkforcePT11+subscribe@list.nist.gov