NIST PRIVACY WORKFORCE PUBLIC WORKING GROUP (PWWG)

Co-Chair: Dylan Gilbert, NIST Privacy Policy Advisor

MEETING MINUTES

Wednesday, February 8, 2022

1:00 p.m. ET – 2:00 p.m. ET

I. INTRODUCTION

The 20th meeting of the National Institute of Standards and Technology (NIST) Privacy Workforce Public Working Group (PWWG) convened on Wednesday, February 8th from 1:00 P.M. - 2:00 P.M. ET virtually via Microsoft Teams. There were 56 attendees.

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, Dylan Gilbert, welcomed attendees and Project Teams Co-Leads and thanked them for their participation. Dylan thanked Meghan Anderson, NIST Privacy Risk Strategist, and the rest of his NIST colleagues for filling in for him while he was out on paternity leave.

The PWWG has three other Co-Chairs for this initiative. Co-Chair Trevor Hughes had to step aside but Doug Forman, Certification Director, International Association of Privacy Professionals (IAPP) kindly agreed to step in and take over Trevor's Co-Chair duties.

II. PWWG UPDATES

A. PROGRESS TO DATE AND OPPORTUNITIES TO IMPROVE

Progress to Date

Two Project Teams have completed their work: Project Team 1: Risk Assessment (ID.RA-P); and Project Team 2: Inventory and Mapping (ID.IM-P).

There are currently three active teams: Project Team 3: Policies, Processes, and Procedures (GV.PO-P, CT.PO-P, CM.PO-P); Project Team 4: Data Processing Ecosystem Risk Management (ID.DE-P); and Project Team 5: Business Environment (ID.BE-P).

Dylan reminded attendees that there are two TKS documents available for reference on the PWWG Google Drive. The TKS Inventory is an alphabetized list of all Tasks, Knowledge, and Skill Statements that were approved for Project Teams 1 and 2. The TKS Mapping document takes those statements and maps

[1] https://www.nist.gov/privacy-framework/privacy-framework

[2] https://www.nist.gov/itl/applied-cybersecurity/nice/nice-framework-resource-center

them to specific Subcategories within the Privacy Framework.

Dylan strongly encouraged team members to review these TKS documents so that they can familiarize themselves with what's been done so far.

Key Challenges and Lessons Learned

The Project Teams have over a year's worth of work completed to date. The NIST Team has identified some key challenges and lessons learned and have set goals for the coming year as well as a new timeline for completing the first phase (i.e., TKS Statement creation) of PWWG work.

1. Conforming TKS Statements

There is a need to standardize the style and tone of TKS Statements. It is very challenging to keep track of subtle distinctions as statements are drafted during their development and approval.

Examples of need for conformance in TKS Statements:

- T011: Coordinate with organizational stakeholders on activities necessary for determining how to assess the effectiveness of privacy controls.
- T062: Engage with organization-defined stakeholders (e.g., through interviews and surveys).
- K001: Knowledge of [organization-selected regulation-defined] roles of system/product/service and component owners or operators.

These statements are subtly but meaningfully different. The first Task Statement is simply about coordinating with organizational stakeholders. The second Task Statement is about engaging with the organization-defined stakeholders. The third Statement is a Knowledge statement, which includes a bracketed organization-selected regulation-defined modifier of roles.

Project Teams 1 and 2, as the first PWWG Project Teams, were operating in a real sandbox environment. Dylan noted that the NIST Team wanted the Teams to have the freedom to explore ideas and ways of framing TKS Statements. The Teams learned that even allowing time for discussion did not necessarily result in consensus on the smallest details.

2. Achieving "Goldilocks" Level of Detail in TKS Statements

There are legitimate arguments for creating detailed TKS Statements as well as for creating higher level statements. A lot of time is spent in Project Team meetings trying to figure out the right balance. There have been very robust debates on this topic.

Examples of high-level versus granular Statements in Risk Assessment Category:

- T006: Apply the privacy risk assessment approach (i.e., quantitative, qualitative, semi-quantitative) to the data actions of the organization’s systems/products/services.
- T066: Evaluate the likelihood that identified problematic data actions of systems/products/services will create problems to individuals by applying the privacy risk assessment approach (i.e., quantitative, qualitative, semi-quantitative).

As Project Team 1 was drafting these TKS Statements, some argued for the more high-level tasks such as in T006. Others argued for more detailed tasks like T066. People were standing their

ground on this. Keeping both Tasks will allow for flexibility for organizations to decide how they want to incorporate these types of risk assessment.

3. Completing Work Quickly/Efficiently

Consensus is a slow process. A great strength of the Working Group is that it is a broad and diverse stakeholder community from all over the world. There are various levels of familiarity with the NIST Privacy Framework and there are differences in the way people go about doing their jobs. There are also new members joining all the time and it takes time to get everyone up to speed.

NIST believes strongly in the consensus process and that is not going to change. The NIST Team has identified steps to improve the process and make the Project Teams' jobs easier. These changes will be necessary in order to meet the goal of completing all Project Teams in 2023.

B. GOALS AND CHANGES FOR 2023

Goal: Complete TKS Statement Creation by January 1, 2024

The 2023 goal for the PWWG is to create and get initial approval for TKS Statements for all remaining Privacy Framework Categories during 2023. The TKS Statements must conform to a standardized style and tone. The final inventory should include TKS Statements from the NICE program that can be mapped, in particular, to the PROTECT-P Function in the Privacy Framework.
The 2024 goal for the PWWG is to open the TKS Inventory up for a broader comment period.

TKS Conformity

Dylan noted that initially the PWWG Team planned to form a Conformance Committee that would be tasked with bringing all of the TKS Statements to standardization and uniformity. The revised plan charges the NIST PWWG Team to take the lead on this task. This will allow the Project Team members to focus on drafting TKS Statements. The Conformance Committee will, in the course of their work, draft an ongoing Style Guide which can applied to the work of future Project Teams.

Remaining Project Teams

- PT6: Risk Management Strategy (GV.RM-P)
- PT7: Awareness and Training (GV.AT-P)
- PT8: Monitoring and Review (GV.MT-P)
- PT9: Data Processing Management (CT.DM-P)
- PT10: Disassociated Processing (CT.DP-P)
- PT11: Data Processing Awareness (CM.AW-P)

Dylan pointed out that there may not be a need for six Project Teams. It may make sense to combine some Categories. The goal will be to find ways to mix and match Categories and Subcategories while leveraging existing TKS Statements to make future Project Teams as efficient as possible. The initial timeline is built on the assumption that there will be six Project Teams.

As mentioned, the PWWG Team will also be leveraging work done by their NICE colleagues in the NICE Framework.

Timeline For Remaining Categories

Dylan shared the following timeline for the proposed completion of the work of the PWWG:

February 1 – April 30, 2023
- Current Project Teams complete their work.
- Project Team 6 - 8 Leads are finalized.
- PT6 – 8 orientations are completed.
- Completed TKS are conformed to standardized rules.
- "Sprint Team" begins incorporating NICE TKS to PWWG.

May 1 – July 31, 2023
- Project Teams 6 – 8 complete their work.
- Project Team 9 – 11 Leads are finalized.
- PT 9 -11 orientations are completed.
- Completed TKS are conformed to standardized rules.
- NICE TKS are fully incorporated into PWWG work.

August 1 – December 31, 2023
- Project Teams 9 – 11 complete their work.
- Completed TKS are reviewed for conformity to rules (NIST Team).
- Process and timeline are finalized for public comments/workshop(s), etc. to finalize TKS in 2024 (NIST Team).

New Project Team Procedures

The PWWG Team has heard feedback from Project Team members and has incorporated some of those ideas to improve the TKS development process.

The first prong of the new approach will involve pre-populating TKS Statements into the Project Team Workbooks. This has already been piloted successfully with Project Team 3. When a new Project Team is launched and begins its work, their TKS Workbook will include already completed and approved Task Statements which come from the completed work of other Project Teams. These will be Statements that can be mapped to the new Project Team's Privacy Framework Category. These TKS Statements will include those that were drafted by other Project Teams that were later determined to be a better fit in a different Privacy Framework Function/Category.

The second change in the PWWG procedures is to have the Project Team Co-Leads and the PWWG Co-Chairs generate the initial set of TKS Statements for Project Team review. The Project Team review will be more akin to a comment adjudication process with the Project Team going through Statement by Statement to fill in details and contextual gaps and adding additional Statements if needed. This should speed up the process by allowing Project Teams to focus less on debating the level of generality or granularity of statements and more on the substance of the Statements themselves.

C. Q&A

Dylan shared some potential questions and answers that he anticipated attendees might have about the new PWWG timeline.

Potential Questions:
Question: Will Project Team Members still be able to suggest new TKS Statements?

- Answer: Yes, both in real time during PT meetings and via comments in the TKS Workbook in between meetings.

Question: Will these changes affect current Project Teams?

- Answer: Except for the April 30th deadline to complete their work, all other changes are optional for current Project Teams.

Question: How do these changes affect the work we've already completed?

- Answer: To the extent that there are inconsistencies among completed TKS Statements (e.g., style, tone, etc.), those will be standardized by the NIST Team.

Dylan open up the meeting for questions.

Open Questions:

Question: How far in advance will the TKS Statements be available for review – days, weeks?

- Answer: They will be complete when the team begins its work. It will all be pre-populated.

Question: I've expressed before, a concern about the different levels of understanding of the Privacy Framework on Project Teams. Not to detract from anybody who wants to contribute, we obviously want as many people involved as possible.
I think it's extremely important, especially when picking Co-Chairs [sic], to make sure they have a sophisticated level of understanding of the Privacy Framework and the subject area. I think, for example, it was the right call to take the subject of biases and give it to the NIST AI team.
There are certain areas where you need more sophisticated knowledge. Disassociated Processing is one of those areas. It is a hard concept to get across. That may be an area where you need to look for specific expertise. One of my concerns early on was, you get a lot of people who are doing well in their corner of the world, but they see the world from their corner.

- Answer: It is certainly a fact that the majority of people that currently work in privacy tend to be lawyers and compliance folks. There is a pretty robust privacy engineering community, but it is relatively smaller.
  Dylan encouraged everyone, to the extent that they know people that are that are working in privacy engineering or have relevant expertise, specifically on the more technical control side, to please let them know about this effort and encourage them to join.

Question: How does the release of NIST Cybersecurity Framework (CSF) 2.0 affect the NICE Framework and what is the timeline for Privacy Framework 2.0?

- Answer: There is no timeline for Privacy Framework updates, although NIST intends to update sometime in the future. The NICE TKS Statements are not specifically aligned with the CSF,

although there is a mapping. It is different from the Privacy Framework in that regard. To the extent that the CSF Core changes, a new mapping from the NICE Framework would likely be necessary.

Question: How do we know which team to join? Years of experience in risk assessments.

- Answer: The NIST PWWG Team will announce when new teams start up. The Risk Assessment and Inventory and Mapping teams completed their work. There are six new teams coming soon. The existing Data Processing Ecosystem Risk Management Project Team (PT4) may be of interest. Any questions should be directed to the PWWG Team.

D. NEXT STEPS - MEMBER SURVEY

The PWWG Team will send out a survey to all members in the next week to gauge specific interest in areas in which people are most interested in working on future Project Teams. If there are suggestions on which Categories can be combined, such as what was done with Project Team 3 (Policies, Processes, and Procedures), there will be an opportunity to share that.

The survey will also include an opportunity for anyone who is interested to sign up for a "sprint team" to help to sort the NICE Framework TKS Statements into the PROTECT-P Subcategories, or into other appropriate Privacy Framework Subcategories.

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.

Co-Lead, Alicia Christensen, VP, General Counsel, Chief Compliance Officer at National Jewish Health, gave an update on the work of PT3. The team has completed their work on TKS Statements for the GV.PO-P1 through GV-PO-P6 Subcategories and have completed review of the Co-Chair comments. They have completed drafting TKS Statements for the CT.PO-P1 and CT.PO-P2 Subcategories.

Alicia noted that one of the challenges faced by the team has been time management and keeping the robust group discussions focused on aligning the Statements with the Subcategory statements. The Co-Leads have found that, for greater efficiency, spending time drafting TKS statements in advance of the group meeting allows more focused discussion during the Project Team meetings.

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.

Dylan Gilbert gave the update for PT4 as the Co-Leads were unavailable to join the meeting.

PT4 has completed drafting TKS Statements for ID.DE-P1 and ID.DE-P2. They are awaiting Co-Chair comments on those Subcategories. PT4 is nearing completion of draft TKS Statements for ID.DE-P3.

Dylan noted PT4 has a large, diverse, global group of members who have different ideas about the work that needs to be done based on the area in which they work and which laws and regulations they may be subject to. This can create a challenge for the team in terms of the discussion and debate around how best to frame some of the Tasks, Knowledge, and Skills and how to keep them agnostic to any law or sector. The required level of granularity also often provides a challenge.

The goal for PT4 for February is to complete ID.DE-P3 and begin drafting Statements for ID.De-P4.

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.

Dylan Gilbert gave the update for PT5 as the Co-Leads were unavailable to join the meeting.
PT5 has completed draft TKS Statements for Subcategory ID.BE-P1 and have submitted them for PWWG Co-Chair review.

Dylan noted that one of the challenges for PT5 is the debate around who the TKS Statements should

be targeted towards: an audience of privacy professionals, or the organizational workforce writ large.

The February goal for PT5 is to complete drafting TKS Statements for Subcategory ID.BE-P2.

IV. Q & A

V. NEXT STEPS & UPCOMING MEETINGS

A. NEXT STEPS

The PWWG Team will send out a survey in the week following this meeting to ask the following:

- Future PWWG Project Teams: Surveying interest in subject matter of future Project Teams
- NICE Framework/Protect-P TKS Statements Activity: Sign up for "sprint team" to sort NICE TKS Statements into Protect-P subcategories

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, February 16, 2023 | 1:00pm – 2:00pm ET
- Thursday, March 2, 2023 | 1:00 p.m. – 2:00 p.m. ET

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

- Thursday, February 9, 2023 | 2:00 p.m. – 3:00 p.m. ET
- Thursday, February 23, 2023 | 2:00 p.m. – 3:00 p.m. ET

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

- Tuesday, February 14, 2023 | 1:00 p.m. – 2:00 p.m. ET
- Tuesday, February 28, 2023 | 1:00 p.m. – 2:00 p.m. ET

NIST Privacy Workforce Public Working Group

- The NIST PWWG meets on the 2nd Wednesday of each month.
- Next meeting: Wednesday, March 8, 2023 |1:00 p.m. – 2:00 p.m. 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. 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