NIST PRIVACY WORKFORCE PUBLIC WORKING GROUP (PWWG)

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

MEETING MINUTES
Wednesday, August 11, 2021
1:00 P.M. ET – 2:00 P.M. ET

I. INTRODUCTION

The fourth (4th) meeting of the NIST Privacy Workforce Public Working Group (PWWG) convened on Wednesday, August 11, 2021 from 1:00 P.M. ET - 2:00 P.M. ET virtually via Microsoft Teams.
Co-Chair: Dylan Gilbert, Privacy Policy Advisor, National Institute of Standards and Technology, welcomed and thanked the members for their participation. The Co-Chair provided a brief overview of the agenda that included the PWWG Member Survey, New Business Open Discussion Topics Drop Box, the Task, Knowledge, and Skill (TKS) Statement Review Process 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 MEMBER SURVEY

It was noted that a NIST PWWG Member Survey is currently in development. The survey will capture information that will allow insight and understanding of the composition of the PWWG membership, (i.e., demographically, sectors, expertise, etc.). This is to ensure a balance and knowledgeable stakeholder representation and engagement of the NIST PWWG and its Project Teams. Survey participation is voluntary and will be used for internal NIST PWWG purposes only. The survey will be distributed to the NIST PWWG membership via the mailing list when it is available.

B. NEW BUSINESS "DROP BOX"

The New Business for open discussion topics Drop Box is currently in development. This will be a resource for the NIST PWWG membership to submit Privacy workforce-related topics and issues for discussion during the NIST PWWG Monthly Meeting. This resource will be available on the NIST PWWG Web page and will be distributed to the PWWG mailing list when it is available. Submissions may be submitted at any time and if selected, will be included in the agenda for future meetings.

C. TASK, KNOWLEDGE, AND SKILL (TKS) STATEMENT REVIEW PROCESS

Dylan thanked the Project Team Leads and members of Project Team 1:Risk Assessment (ID.RA-P) and Project Team 2: Inventory and Mapping (ID.IM-P) for their leadership, contributions, and participation in the development of the Task, Knowledge, and Skill (TKS) Statements.
It was noted that both Project Teams are currently in the initial review phase and advised the NIST PWWG membership of the TKS review process and encouraged members with the specified expertise to offer comments. In the coming weeks, the Project Teams will wrap up their review and send their final TKS Statements to the NIST PWWG Co-Chairs for review. Please note the TKS Statement review process below:

- Step 1: Project Teams review and approve TKS Statements via shared Google Sheet.
- Step 2: Co-Chairs will review, approve, or send back with comments to the Project Team(s) for further review and revision.
- Step 3: Upon final review and approval, the Project Team is dissolved, and the next Privacy Framework Category is assigned to a new Project Team.

III. PROJECT TEAM UPDATES

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

Project Team Co-Lead, Lauren Jones Data Privacy & Protection Counsel, FINRA, provided a brief background and status of Project Team 1: Risk Assessment (ID.RA-P) Task, Knowledge, and Skill (TKS) Statements. Project Team Co-Lead, Lisa McKee Senior Manager Security and Data Privacy, Protiviti was unable to join.

The Team is tasked with the development of the TKS Statements for five (5) Subcategories from the NIST Privacy Framework Core V1[1].

- **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.

The Project Team Co-Lead provided examples of how the team members reviewed their TKS Statements for ID.RA-P1 and their discussion points from their August meeting.

Project Team 1 focused their TKS Statement review process on identifying Risk Assessment inputs and outputs and keeping the Statements simple and focused. Other discussions included recognizing the challenge of dependencies and determining how to include them and how they fit together overall within the NIST Privacy Framework. Below are examples TKS Statements in review:

> 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).

[1] NIST Privacy Framework Core

- Proposed Task 1: Identify personal data
- Proposed Task 2: Classify personal data
- Decision: Remove from consideration (Rationale: Risk assessment input)
- General rule: When considering dependencies among TKS Statements, if in doubt, include

The example TKS Statement below is an indication of the simplification and focus aspect of the review process, which determines whether a Task is too focused or too broad. If the Task is too broad, then the Task is broken down into three (3) separate Tasks.

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).

- Proposed Task: Identify groups of individuals put at risk by systems/products/services
- Task Version 2: Identify categories of individuals put at risk by systems/products/services
- Task Version 3: Identify categories of individuals put at risk by systems

Reminded the NIST PWWG membership that the current project review schedule is in the Project Team 1: Risk Assessment (ID.RA-P) Google Drive. In addition, the Project Team Co-Lead encouraged NIST PWWG members who are interested to join the NIST PWWG Project Team 1 mailing list.

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

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

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 V1[2].

- **IDENTIFY-P (ID-P):** Develop the organizational understanding to manage privacy risk for individuals a rising 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.

[2] NIST Privacy Framework Core

- **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.

The Project Team Co-Lead stated that the Project Team has met four (4) times and have reviewed all eight (8) ID.IM Subcategories. Their TKS review process consisted of following principles which are color coded within the TKS Google Sheet:

- **Don't duplicate basic controls found in other control frameworks like NIST CSF or SOC:** TKS Taxonomy is intended to be incremental to basic controls, rather than a place to document step-by step how to put basic controls in place (e.g. asset inventory)
- **No Project Planning:** No need to break out Task Statements into entire detailed project plan or apply detailed System Development Lifecycle (SDLC)
- **Unique:** If T, K or S is not unique to that Subcategory outcome/activity, probably doesn't belong (e.g., "build support in your org;" "identify stakeholders")
- **Within Scope:** Do not expand the scope of the Subcategory

The Project Team Co-Lead provided examples of how the team members reviewed their TKS Statements for ID.IM-(P1, P3, P6, and P7) and their discussion points from their August meeting. During the initial review process, the Project Team discussed how the separation of duties, the categorization of individuals, and addressing compounding of the TKS Statements were topics to consider. Example TKS Statements were provided as noted below:

- **Example: ID.IM-P1: Systems/products/services that process data are inventoried.**
  - Proposed 6/20
    - Task: Identify and document all systems/products/services that process data.
  - Proposed 7/12, approved 8/9
    - Task: Identify all systems that process data
    - Likewise broke out 6 tasks to respect "no compounding" guideline
  - Proposed 7/26, not approved 8/9
    - Task: Identify separation-of-duties risk between roles
    - Not unique to this subcategory, goes beyond scope

- **Example: ID.IM-P3: Categories of individuals (e.g., customers, employees or prospective employees, consumers) whose data are being processed are inventoried.**
  - Proposed 6/20, initially approved 8/9:
    - Task: Identify categories of individuals (e.g., customers, employees or prospective employees, consumers) whose data are being processed
  - Proposed 7/26, initially approved 8/9 as an additional Task:
    - Task: Identify those categories of individuals described in regulation where the rules for processing their information differ.

- **Example: ID.IM-P6: Data elements within the data actions are inventoried.**
  - Proposed 6/20, initially approved 8/9:
    - Task: Identify data elements within the data actions

        - Task: Document data elements within the data actions
    - Proposed 7/26, under discussion 8/9:
        - (Phase 3) Task: Determine whether you want to collect data element information for all systems or just those that store or process personal data
            - Determine the requirements you will place on those responsible for providing information
            - Note that providing information on systems that don't store personal information may be harder to persuade people to provide

- **Example: ID.IM-P7: The data processing environment is identified (e.g., geographic location, internal, cloud, third parties)**
    - Proposed 6/21, initially approved 8/9
        - Task: Document the data processing environment(s) (e.g., geographic location, internal, cloud, third parties).
        - Knowledge: Knowledge of data processing environment
        - Skill: Skill in documenting different data processing environments
    - Proposed 7/26, not approved 8/9 (beyond scope)
        - Task: Identify data processing environment who has the data, how long you keep the data, who wipes the data
        - Knowledge: Knowledge of pre-processing environment
        - Skill: Skill in documenting who has the data, how long you keep the data, and who wipes the data.

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

IV. NEXT STEPS & UPCOMING MEETINGS

A. NEXT STEPS

- Project Teams will continue to review and finalize TKS Statements and submit to the NIST PWWG Co-Chairs for review and comment.
- NIST PWWG Member Survey will be finalized and distributed in the next coming weeks via the mailing list.
- New Business Open Discussion Topics Drop Box will be available on the NIST PWWG web page and an announcement will be distributed to the mailing list when its available.

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, August 18, 2021 — 5:00pm ET – 6:00pm ET
    - Thursday, September 2, 2021 — 11:00am ET – 12:00pm ET
2) **Project Team 2: Inventory and Mapping (ID.IM-P)**
    - Monday, August 23, 2021 — 12:00pm ET – 1:00pm ET
    - September, TBD (Will be rescheduled due to Labor Day)
3) **NIST Privacy Workforce Public Working Group**
    - Wednesday, September 8, 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