



NIST Privacy Workforce Public Working Group

Meeting #4

Wednesday, August 11, 2021

INTRODUCTION



PWWG UPDATES

COMING SOON: PWWG MEMBER SURVEY

- Goals:
 - Better understand PWWG membership composition
 - Help ensure balanced, broad, knowledgeable stakeholder representation and engagement
- **Participation is voluntary**
- **Information used for internal NIST purposes only**
- Google form circulated via PWWG mailing list

COMING SOON: NEW BUSINESS “DROP BOX”

- Purpose: Members submit suggested topics for open discussion at PWWG monthly meetings “on demand”
- Accessible via PWWG web page
- May be submitted at anytime
- Privacy workforce-related topics and issues only, please

TKS STATEMENTS REVIEW PROCESS

- Step 1: Project Teams review and approve TKS Statement via shared doc
 - **Both Project Teams at review stage. Now's the time to weigh in!**
- Step 2: Co-Chairs review and approve or send back to Project Team(s) for further revision
- Step 3: Upon final review and approval, Project Team is dissolved and assigned to the next Privacy Framework Category

PROJECT TEAM UPDATES

PROJECT TEAM 1:

Risk Assessment (ID.RA-P)

Project Team 1: Risk Assessment (ID.RA-P)

Team Co-Leads



Lauren Jones
Data Privacy & Protection Counsel,
FINRA



Lisa McKee
Senior Manager Security and Data Privacy,
Protiviti

Project Team 1: Risk Assessment (ID.RA-P)

AUG Meeting Recap: Status



Pencils Down: Review of Risk-
Assessment Sub-categories

Project Team 1: Risk Assessment (ID.RA-P)

AUG Meeting Recap: Overview

NIST PRIVACY FRAMEWORK CORE

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 1: Risk Assessment (ID.RA-P)

AUG Meeting Recap: Discussion Points



Risk Assessment Inputs and Outputs



Simplify and Focus!

Project Team 1: Risk Assessment (ID.RA-P)

Task, Knowledge, and Skill (TKS) Statements

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

Project Team 1: Risk Assessment (ID.RA-P)

Task, Knowledge, and Skill (TKS) Statements – P1

Example: 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

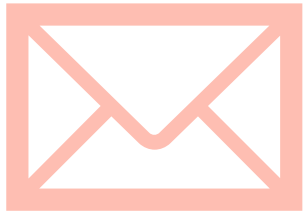
Project Team 1: Risk Assessment (ID.RA-P)

Recurring Meetings

- Every 1st Thursday of the month | 11:00AM - 12:00 PM ET
- Every 3rd Wednesday of the month | 5:00PM – 6:00PM ET
 - Next meeting
 - **Wednesday, August 18, 2021 | 5:00PM – 6:00PM ET**

Project Team 1: Risk Assessment (ID.RA-P)

Mailing List Sign-Up



(PrivacyWorkforcePT1+subscribe@list.nist.gov)

PROJECT TEAM UPDATES

PROJECT TEAM 2:

Inventory and Mapping (ID.IM-P)

Project Team 2: Inventory and Mapping (ID.IM-P)

Team Co-Leads



Dr. Sarah Lewis Cortes
Privacy Engineering, Netflix



Mary Potter
Director of Privacy and Research Data
Protections, Virginia Tech

Project Team 2: Inventory and Mapping (ID.IM-P)

Overview

Project Team 2:

- Task, Knowledge, and Skill (TKS) Statements
 - Subcategories

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 2: Inventory and Mapping (ID.IM-P)

Progress Update

- We have reviewed all 8 ID.IM Subcategories multiple times (6/21, 7/12, 7/26, 8/9)
- Green, Yellow, Red, Blue approval status: Proposals & comments open for 4 weeks, now closed, approved/rejected after 2 more weeks
- Proposed core or “floor” TKS that need not be repeated in each TKS

Project Team 2: Inventory and Mapping (ID.IM-P)

Progress Update – TKS Evaluation Principles

- Proposed evaluation principles for each TKS:
 - **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

Project Team 2: Inventory and Mapping (ID.IM-P)

Task, Knowledge, and Skill (TKS) Statements – P1

Example: ID.IM-P1: Systems/products/services that process data are inventoried.

- Proposed 6/20 T: Identify and document all systems/products/services that process data
- Proposed 7/12, approved 8/9 T: Identify all systems that process data
 - Likewise broke out 6 tasks to respect “no compounding” guideline
- Proposed 7/26, not approved 8/9 T: Identify separation-of-duties risk between roles
 - Not unique to this subcategory, goes beyond scope

Project Team 2: Inventory and Mapping (ID.IM-P) Task, Knowledge, and Skill (TKS) Statements – P3

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.

Project Team 2: Inventory and Mapping (ID.IM-P) Task, Knowledge, and Skill (TKS) Statements – P6

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
 - 1. Determine the requirements you will place on those responsible for providing information
 - 2. Note that providing information on systems that don't store personal information may be harder to persuade people to provide

Project Team 2: Inventory and Mapping (ID.IM-P)

Task, Knowledge, and Skill (TKS) Statements – P7

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
 - T: Document the data processing environment(s) (e.g., geographic location, internal, cloud, third parties).
 - K: Knowledge of data processing environment
 - S: Skill in documenting different data processing environments
- Proposed 7/26, not approved 8/9 (beyond scope)
 - T: Identify data processing environment who has the data, how long you keep the data, who wipes the data
 - K: Knowledge of pre-processing environment
 - S: Skill in documenting who has the data, how long you keep the data, and who wipes the data

Project Team 2: Inventory and Mapping (ID.IM-P)

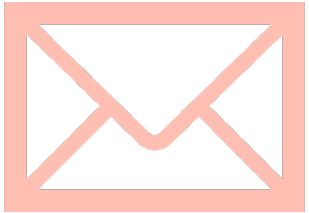
Recurring Meetings

Biweekly on Mondays from 12:00 PM ET to 1:00 PM ET

- **Next meeting is on Monday, August 23, 2021**

Project Team 2: Inventory and Mapping (ID.IM-P)

Mailing List Sign-Up



(PrivacyWorkforcePT2+subscribe@list.nist.gov)



**NEXT STEPS &
UPCOMING MEETINGS**

Privacy Workforce Public Working Group

Next Steps

- Project Teams will review and finalize TKS Statements and submit to Co-Chairs for review
- Member survey circulated
- New business drop box added to web page

Privacy Workforce Public Working Group

Upcoming Meetings

- 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**
- 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)**
- NIST Privacy Workforce Public Working Group
 - **Wednesday, September 8, 2021 — 1:00pm ET – 2:00pm ET**

* For updated meeting schedules see the [PWWG web page](#).

Privacy Workforce Public Working Group Web Page

How to get involved:

[Privacy Workforce Public Working Group | NIST](#)

Privacy Workforce Public Working Group

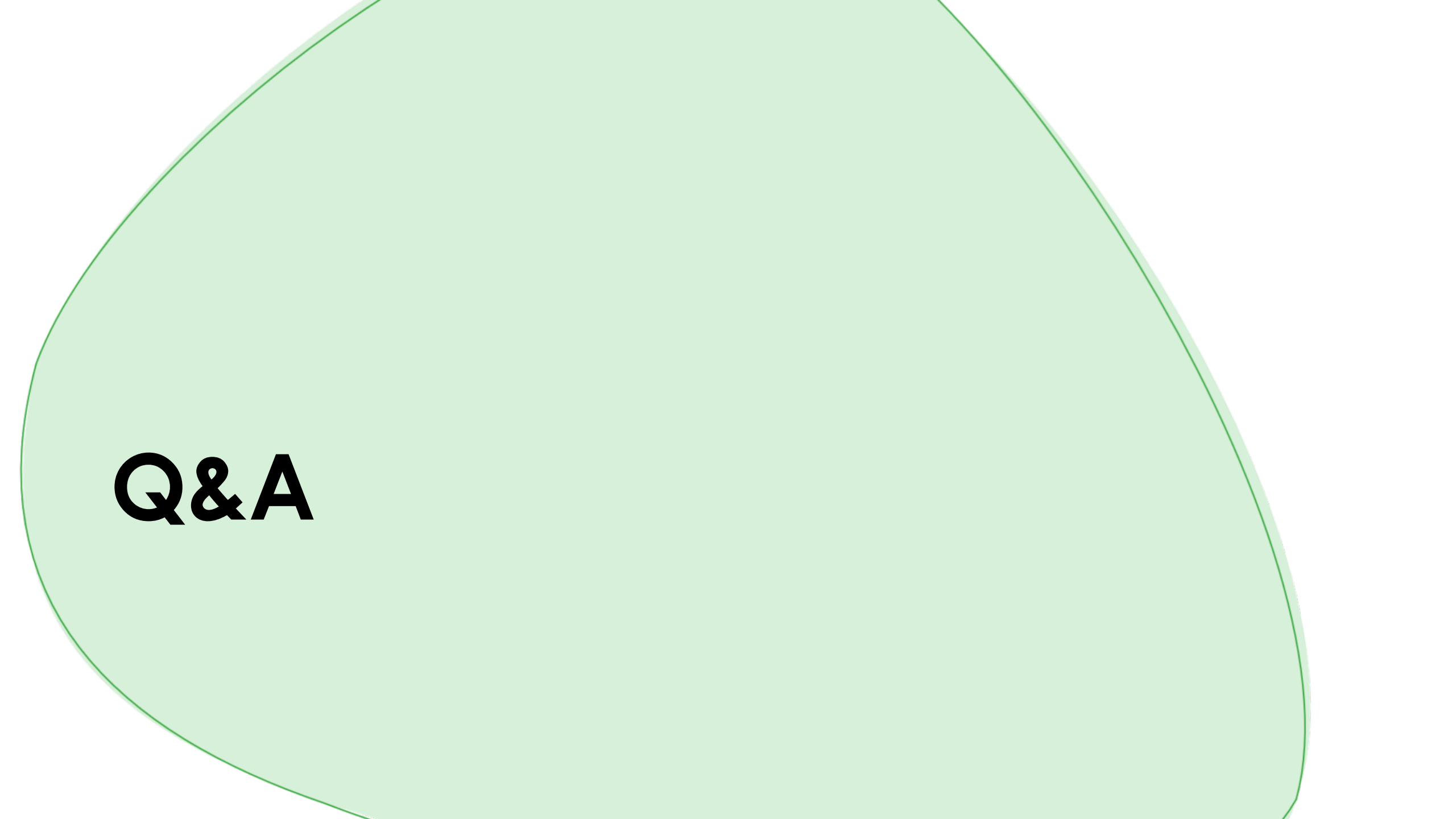
Mailing Lists

- PWWG (PrivacyWorkforceWG@list.nist.gov)
- Project Team (PT1) (PrivacyWorkforcePT1@list.nist.gov)
- Project Team 2 (PT2) (PrivacyWorkforcePT2@list.nist.gov)
- **All mailing lists are moderated**

Privacy Workforce Public Working Group

Troubleshooting

- Email questions to pwwg@nist.gov



Q&A