



NIST Privacy Workforce Public Working Group

Meeting #11

Wednesday, March 9, 2022

INTRODUCTION



PWWG UPDATES

PWWG Updates

Project Team 2: Inventory and Mapping

Through the finish line!*

*Basically...



PWWG Updates

Project Team 3: Policies, Processes, and Procedures

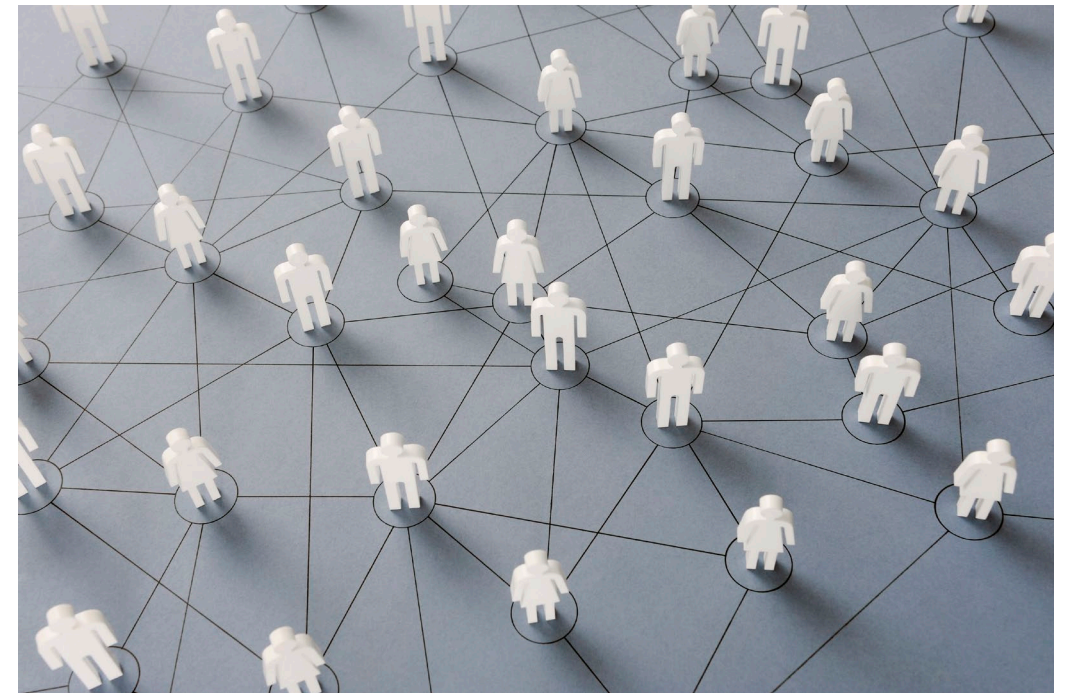
- Off to the races!
- TKS Statements under development



PWWG Updates

Project Team 4: Data Processing Ecosystem Risk Management

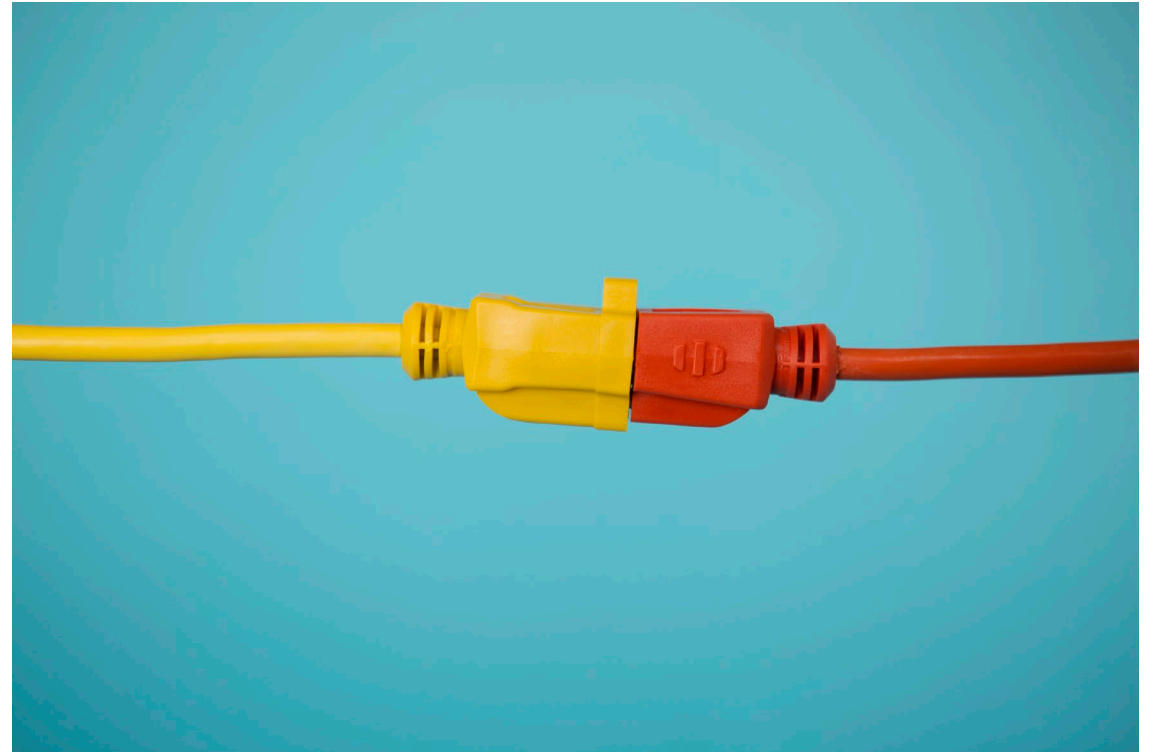
- Co-Leads selected (introductions after Project Team updates)
- First meeting, March 10 (3:00PM – 4:00PM ET)



PWWG Updates

Privacy Framework >< PWWG TKS Mapping

- Mapping of completed TKS Statements to Privacy Framework Core Subcategories
- Read-only document, accessible to PWWG members via shared Google Drive
- Targeting week of March 21st for release



PWWG Updates

Co-Chairs TKS Statement Review Update

- Reviewing Project Team 1 TKS Statements for ID.RA-P1, P2, P3 and P4
- Next Co-Chairs TKS Review: March 24, 2022
- Implemented new policy of open invitation for Project Team Leads to join review sessions

PROJECT TEAM UPDATES

PROJECT TEAM 1:

Risk Assessment (ID.RA-P)

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

Team Co-Leads



Lauren Jones
Privacy Counsel, Surescripts, LLC



Dr. Lisa McKee
Senior Manager Security and Data Privacy, Protiviti

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

Task, Knowledge, Skill Statements (TKS)

Project Team 1:

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

Subcategory	Description
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)

Progress Update

- Project Team's goals for the March work period
 - The team is currently working on last Subcategory ID.RA-P5
- Accomplishments
 - Completed Subcategory ID.RA-P4 and is in Co-Chair review
- Challenges/lessons learned

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, March 16, 2022, | 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)

Task, Knowledge, Skill Statements (TKS)

- **Project Team 2:**
 - **Task, Knowledge, and Skill (TKS) Statements**

Subcategory	Description
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 -1

Goals for March work period

- Closeout Team 2

February 2022 Accomplishments

- Review of final comments from the PWWG co-chairs
- Incorporated changes and updates from co-chairs and team members

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

Progress Update -2

Acknowledgements

- Thank you to all Team 2 participants for your thoughtful contributions and thought-provoking comments.
- Thank you to our PWWG Co-chairs for your guidance and oversight.
- Thank you to our coordinators who kept us organized and on track.
- You were amazing to work with.

PROJECT TEAM UPDATES

PROJECT TEAM 3:

**Policies, Processes, and Procedures
(GV.PO-P, CT.PO-P, CM.PO-P)**

Project Team 3: Policies, Processes, and Procedures (GV.PO-P, CT.PO-P, CM.PO-P)

Team Co-Leads



Amin Ali

GRC Program Manager &
Cybersecurity PMO Lead
Motorola Solutions



Dan LoPresto

Director, Privacy Compliance
University of Central Florida
(UCF)



Nandita Rao Narla

Senior Privacy Program Manager
Door Dash

Project Team 3: Policies, Processes, and Procedures (GV.PO-P, CT.PO-P, CM.PO-P)

Scope of Work

- **NIST PWWG Project Team 3: Policies, Processes, and Procedures**

- **Project Team Abbreviation: (PT3)**

1) Function: GOVERN-P (GV-P):

- Category (GV.PO-P): Governance Policies, Processes, and Procedures
- Subcategories (6): GV.PO-P1 through GV.PO-P6

2) Function: CONTROL-P (CT-P):

- Category (CT.PO-P): Data Processing Policies, Processes, and Procedures
- Subcategories (4): CT.PO-P1 through CT.PO-P4

3) Function: COMMUNICATE-P (CM-P):

- Category (CM.PO-P): Communication Policies, Processes, and Procedures
- Subcategories (2): CM.PO-P1 and CM.PO-P2

Project Team 3: Policies, Processes, and Procedures (GV.PO-P, CT.PO-P, CM.PO-P)

Scope of Work: Privacy Framework

PROJECT TEAM 3 CATEGORIES		
Function	Category	Subcategory
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.	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.	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.
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 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.	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.
COMMUNICATE-P (CM-P): Develop and implement appropriate activities to enable organizations and individuals to have a reliable understanding and engage in a dialogue about how data are processed and associated privacy risks.	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.	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 3: Policies, Processes, and Procedures (GV.PO-P, CT.PO-P, CM.PO-P)

Progress Update

Working on drafting 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.
- All meeting minutes can be accessed on the [Project Team 3 - Google Drive](#).

Project Team 3: Policies, Processes, and Procedures (GV.PO-P, CT.PO-P, CM.PO-P)

Next Steps

- PT3 will continue brainstorming TKS Statements at the next meeting.

Project Team 3: Policies, Processes, and Procedures (GV.PO-P, CT.PO-P, CM.PO-P)

Recurring Meetings

Biweekly on Thursdays from 1:00 PM ET to 2:00 PM ET

Next meeting:

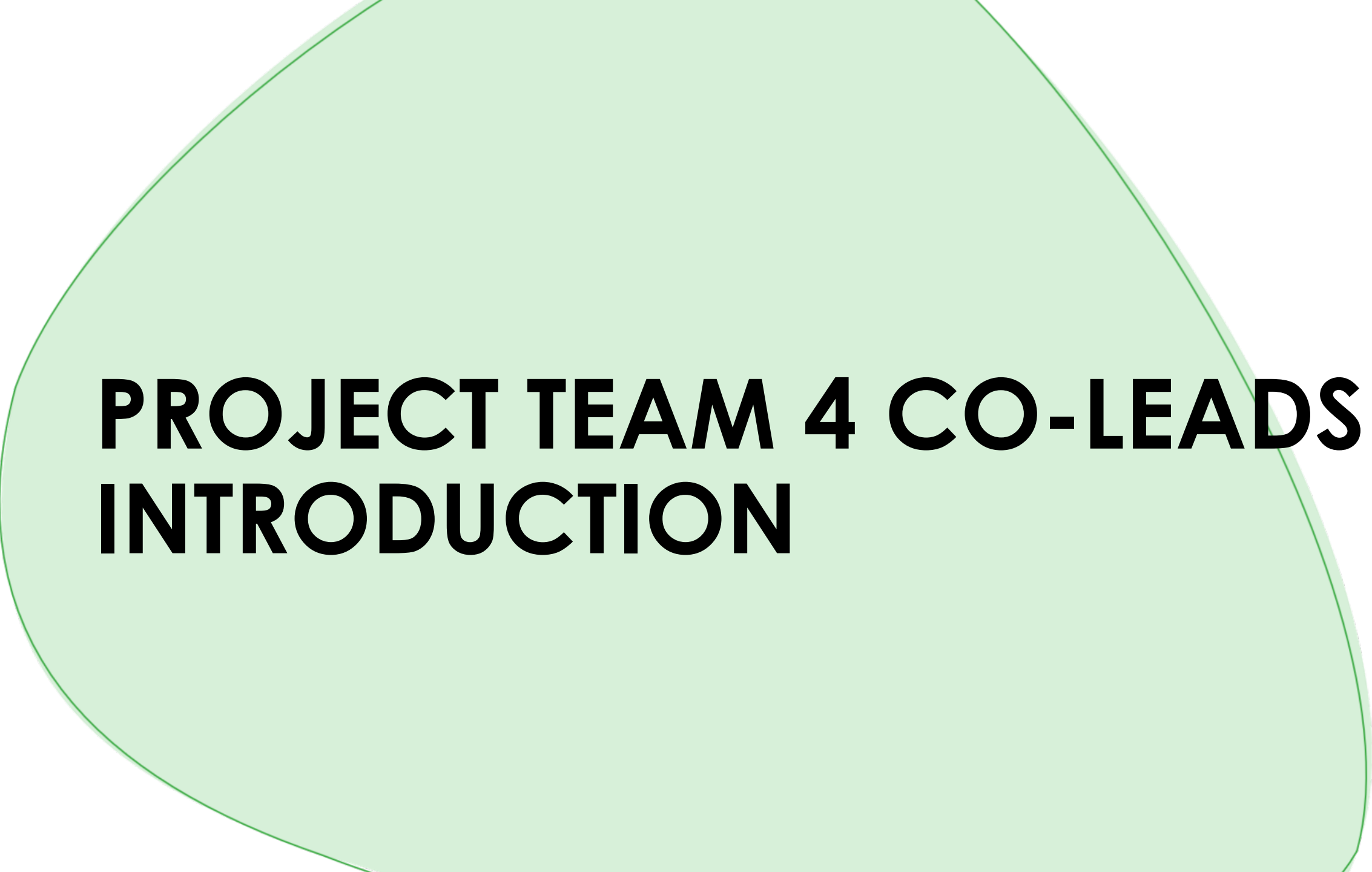
Thursday, March 17, 2022

Project Team 3: Policies, Processes, and Procedures (GV.PO-P, CT.PO-P, CM.PO-P)

Mailing List Sign-Up



PrivacyWorkforcePT3+subscribe@list.nist.gov

A light green, abstract, teardrop-shaped graphic element with a thin green outline, positioned on the left side of the slide. It contains the main title text.

PROJECT TEAM 4 CO-LEADS INTRODUCTION

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

Team Co-Leads



Tahir Latif

Head of Practice - Data Protection,
Artificial Intelligence and Analytics
(APAC & EMEA) Cognizant
Worldwide



Paul Lanois

Director, FieldFisher



Anne Connell

Senior Cybersecurity Engineer,
Carnegie Mellon University



**NEXT STEPS &
UPCOMING MEETINGS**

Privacy Workforce Public Working Group

Next Steps

- Project Team 1 works with Co-Chairs to finalize TKS Statements
- PT3 continues to develop TKS Statements
- PT4 begins
- NIST finalizes PF/TKS mapping

Privacy Workforce Public Working Group

Upcoming Meetings

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

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

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)
- Project Team 3 (PT3) (PrivacyWorkforcePT3@list.nist.gov)
- Project Team 4 (PT4) (PrivacyWorkforcePT4@list.nist.gov)
- **All mailing lists are moderated**

Privacy Workforce Public Working Group

Troubleshooting

- Email questions to pwwg@nist.gov



Q & A