NIST Privacy Workforce Public Working Group

Meeting #17
Wednesday, September 14, 2022

INTRODUCTION

PWWG Co-Chairs

Dylan Gilbert
Privacy Policy Advisor
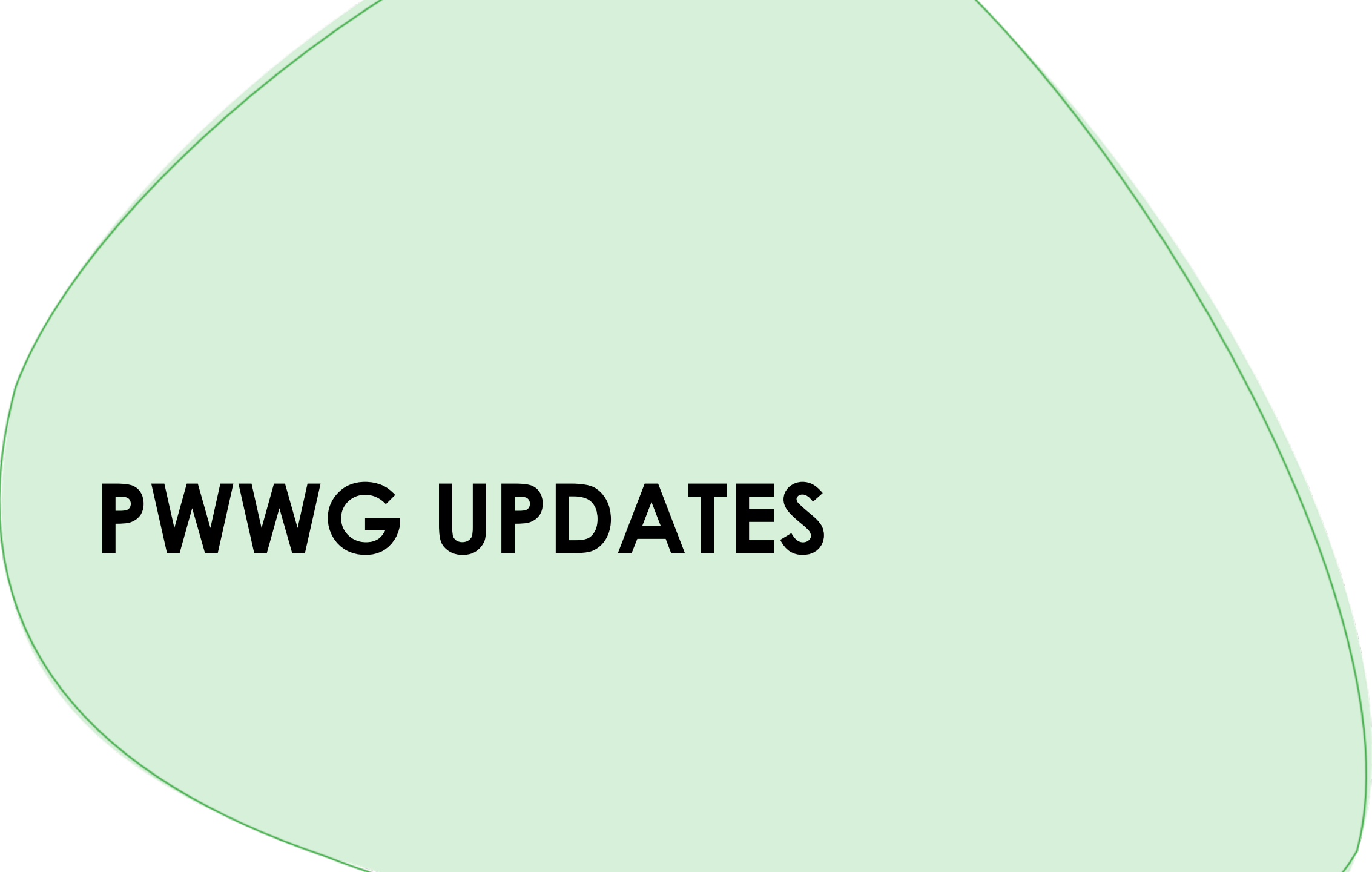*National Institute of Standards and Technology*

Trevor Hughes, CIPP
President & CEO
International Association of Privacy Professionals

Mary N. Chaney, Esq., CISSP, CIPP/US
Managing Attorney
The Law Offices of Mary N. Chaney, PLLC

Melanie Ensign
Founder & CEO
Discernable, Inc.

PWWG UPDATES

PWWG Updates
PT1: RISK ASSESSMENT (ID.RA-P)

Thanks to all involved!

PWWG Updates
PT1: RISK ASSESSMENT – FINAL TKS STATEMENTS

- ~ 200 Task, Knowledge, and Skill Statements

- Mixture of high-level and detailed tasks

- Open for further comments when PWWG process completes

PWWG Updates
FINAL TKS STATEMENTS

Inventory Document

Mapping Document

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
Director of Governance, Risk,
Compliance and Privacy, Hudl

Project Team 1: Risk Assessment (ID.RA-P)
Task, Knowledge, Skill Statements (TKS)

Project Team 1:
- **ID.RA-P 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 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

Dan LoPresto
Director, Privacy Compliance
University of Central Florida (UCF)

Nandita Rao Narla
Senior Privacy Program Manager
DoorDash

Alicia Christensen, JD, MS, CIPP/US, CIPM
VP, General Counsel, Chief Compliance Officer at National Jewish Health
Principal Advisor, Frame Privacy Group

NIST PWWG Project Team 3 (PT3):
          Policies, Processes, and Procedures

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

NIST Privacy Framework Core		
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
		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
		CT.PO-P2: Policies, processes, and procedures for enabling data review, transfer, sharing or disclosure,
		CT.PO-P3: Policies, processes, and procedures for enabling individuals' data processing preferences and
		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

Planned work for September/October:

- PT3 is currently reviewing and discussing the Co-Chair comments for the TKS Statements for GV.PO-P1- GC.PO-P6: Governance Policies, Processes, and Procedures.

- The team will begin drafting TKS Statements for subcategories in CT.PO-P: Data Processing Policies, Processes, and Procedures.

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 EDT to 2:00 PM EDT

Next meeting:

Thursday, September 15, 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

PROJECT TEAM UPDATES

PROJECT TEAM 4:
Data Processing Ecosystem
Risk Management (ID.DE-P)

Project Team 4: Data Processing Ecosystem (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,
Software Engineering Institute
Carnegie Mellon University

Project Team 4: Data Processing Ecosystem (ID.DE-P)
Task, Knowledge, Skill Statements (TKS)

Project Team 4 (PT4):
- **Task, Knowledge, and Skill (TKS) Statements**
  - **Subcategories**

Subcategory	Description
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.

Project Team 4: Data Processing Ecosystem (ID.DE-P)
Progress Update

Currently working on drafting TKS statements for :

- **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.

Project Team 4: Data Processing Ecosystem (ID.DE-P)
Progress Update - 2

Goals for this work period:

- Complete drafting TKS statements for ID.DE-P2 and send to Co-Chairs for review.

- Continue the development of TKS statements for the ID.DE-P subcategories

Project Team 4: Data Processing Ecosystem (ID.DE-P)
Recurring Meetings

Two meetings each month:

- 1st & 3rd Thursday of the month | 2:00 PM to 3:00 PM EDT

- Next meeting:

  Thursday, September 15, 2022 | 2:00 PM – 3:00 PM EDT

Project Team 4: Data Processing Ecosystem (ID.DE-P)
Mailing List Sign-Up

PrivacyWorkforcePT4+subscribe@list.nist.gov

PROJECT TEAM UPDATES

PROJECT TEAM 5:
Business Environment (ID.BE-P)

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

Anshu Gupta
VP, Security and Privacy, CISO
Span.io

Brandi M. Bennett, CIPP-US
Data Privacy and Security
Attorney

Project Team 5: Business Environment (ID.BE-P)
Task, Knowledge, Skill Statements (TKS)

Project Team 5 (PT5):
- ### Task, Knowledge, and Skill (TKS) Statements
  - #### Subcategories

Subcategory	Description
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.

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

Two meetings each month:

- Biweekly on Tuesdays | 1:00 PM to 2:00 PM EDT

- Next meeting:

  Tuesday, September 27, 2022 | 1:00 PM – 2:00 PM EDT

Project Team 5: Business Environment (ID.BE-P)
Mailing List Sign-Up

PrivacyWorkforcePT5+subscribe@list.nist.gov

NEXT STEPS & UPCOMING MEETINGS

Privacy Workforce Public Working Group
Next Steps

- NIST PWWG team finalizes TKS inventory and mapping documents with PT1 material

- PT3 finalizes TKS Statements for GV.PO-P

- PT4 reviews Co-Chair comments on TKS Statements for ID.DE-P2

- PT5 continues drafting TKS Statements for ID.BE-P1

Privacy Workforce Public Working Group
Upcoming Meetings

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

Project Team 3: Policies, Processes, and Procedures (GV.PO-P, CM.PO-P, CT.PO-P)
Thursday, September 15, 2022 | 1:00pm – 2:00pm EDT

Project Team 4: Data Processing Ecosystem Risk Management (ID.DE-P)
Thursday, September 15, 2022 | 2:00pm – 3:00pm EDT

Project Team 5: Business Environment (ID.BE-P)
Tuesday, September 27, 2022 | 1:00pm – 2:00pm EDT

NIST Privacy Workforce Public Working Group
Wednesday, October 12, 2022 |1:00pm – 2:00pm EDT

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

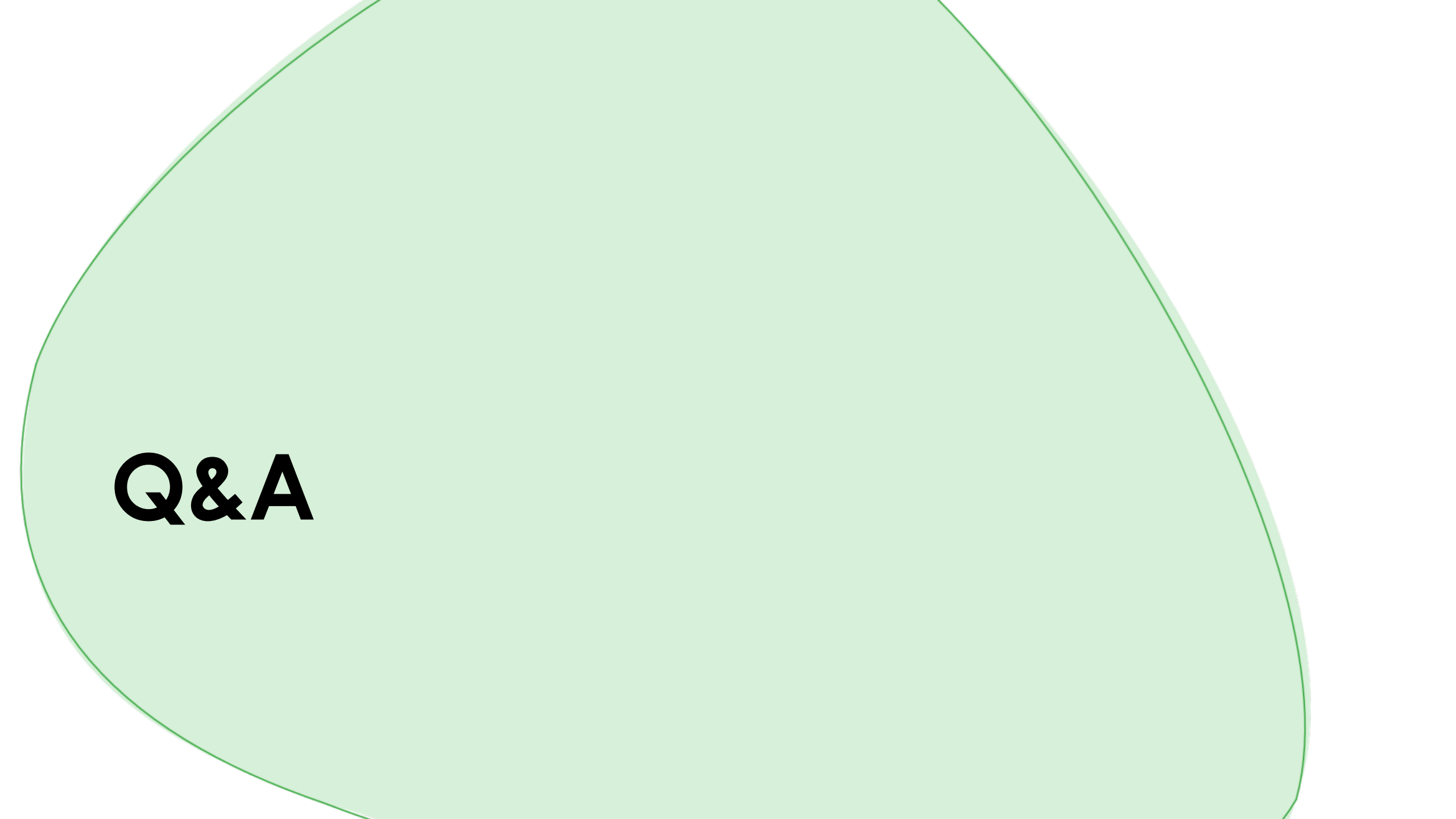# Privacy Workforce Public Working Group
Join Our Mailing Lists

- Privacy Workforce Working Group (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

- **All mailing lists are moderated**

Privacy Workforce Public Working Group
Troubleshooting

- Email questions to pwwg@nist.gov

Q&A