NIST Privacy Workforce Public Working Group

Meeting #29

Wednesday, November 8, 2023

NIST NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY U.S. DEPARTMENT OF COMMERCE

INTRODUCTION

PWWG Co-Chairs

Dylan Gilbert
Privacy Policy Advisor
National Institute of Standards and Technology

Doug Forman
Certification Director
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

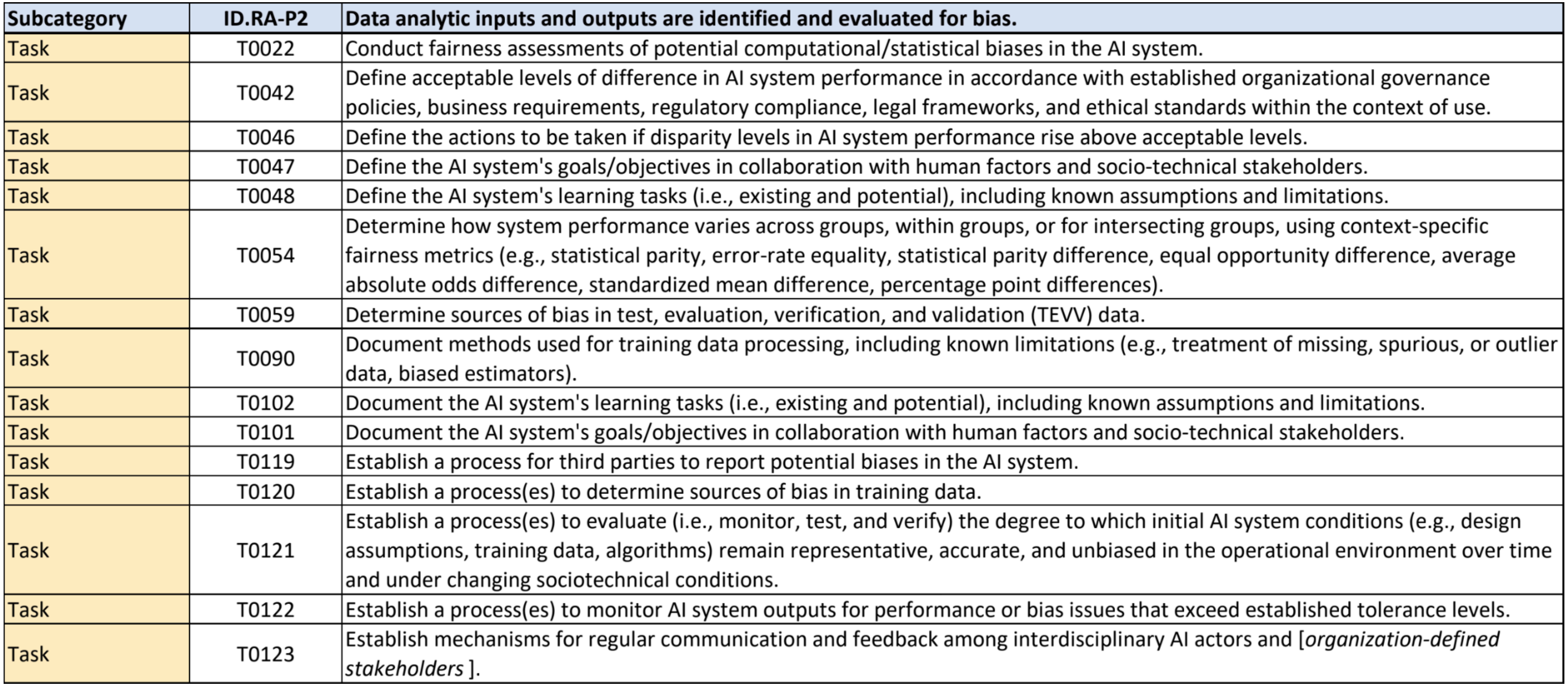
TKS Compilation Documents – Version 6

234 TASK STATEMENTS

206 KNOWLEDGE STATEMENTS

234 SKILL STATEMENTS

PWWG Updates
TKS Compilation Documents – Version 6



Subcategory	ID.RA-P2	Data analytic inputs and outputs are identified and evaluated for bias.
Task	T0022	Conduct fairness assessments of potential computational/statistical biases in the AI system.
Task	T0042	Define acceptable levels of difference in AI system performance in accordance with established organizational governance policies, business requirements, regulatory compliance, legal frameworks, and ethical standards within the context of use.
Task	T0046	Define the actions to be taken if disparity levels in AI system performance rise above acceptable levels.
Task	T0047	Define the AI system's goals/objectives in collaboration with human factors and socio-technical stakeholders.
Task	T0048	Define the AI system's learning tasks (i.e., existing and potential), including known assumptions and limitations.
Task	T0054	Determine how system performance varies across groups, within groups, or for intersecting groups, using context-specific fairness metrics (e.g., statistical parity, error-rate equality, statistical parity difference, equal opportunity difference, average absolute odds difference, standardized mean difference, percentage point differences).
Task	T0059	Determine sources of bias in test, evaluation, verification, and validation (TEVV) data.
Task	T0090	Document methods used for training data processing, including known limitations (e.g., treatment of missing, spurious, or outlier data, biased estimators).
Task	T0102	Document the AI system's learning tasks (i.e., existing and potential), including known assumptions and limitations.
Task	T0101	Document the AI system's goals/objectives in collaboration with human factors and socio-technical stakeholders.
Task	T0119	Establish a process for third parties to report potential biases in the AI system.
Task	T0120	Establish a process(es) to determine sources of bias in training data.
Task	T0121	Establish a process(es) to evaluate (i.e., monitor, test, and verify) the degree to which initial AI system conditions (e.g., design assumptions, training data, algorithms) remain representative, accurate, and unbiased in the operational environment over time and under changing sociotechnical conditions.
Task	T0122	Establish a process(es) to monitor AI system outputs for performance or bias issues that exceed established tolerance levels.
Task	T0123	Establish mechanisms for regular communication and feedback among interdisciplinary AI actors and [*organization-defined stakeholders*].

PWWG Updates
TKS Compilation Documents – Version 6

TKS Compilation Inventory

TKS Compilation Mapping

PWWG Updates
Orientation Video

- On demand for all PWWG members
- Finalizing details and then will be posted on webpage
- Available very soon

PWWG Updates
TKS Baseline

- Foundational Task, Knowledge, and Skill Statements that are applicable across the Privacy Framework Core
- Will be included somewhere in the taxonomy, likely front matter and/or an appendix
- New tab in the PT9 – PT11 Workbooks with ~40 TKS Statements

PROJECT TEAM UPDATES

Project Team 6: Risk Management Strategy (GV.RM-P)

Co-Leads

Dana Garbo
Chief Privacy Officer,
Medline Industries

James Koons
Founding Partner, Data Privacy
& Security Advisors

Project Team 6: Work Assignment

Function: 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.

Category: Risk Management Strategy (GV.RM-P): The organization’s priorities, constraints, risk tolerances, and assumptions are established and used to support operational risk decisions.

Subcategory	**Description**
GV.RM-P1	Risk management processes are established, managed, and agreed to by organizational stakeholders.
GV.RM-P2	Organizational risk tolerance is determined and clearly expressed.
GV.RM-P3	The organization’s determination of risk tolerance is informed by its role(s) in the data processing ecosystem.

Project Team 6: Risk Management Strategy (GV.RM-P)
Progress Update

- **Current Status**
  - Completed review of Co-Chair feedback for TKS Statements in GV.RM-P1.

- **Goals for this work period:**
  - Complete review of TKS Statements for GV.RM-P3
  - Review Co-Chair feedback for GV.RM-P2 (Co-Leads)

The Co-Leads encourage all members to continue to leave comments on the TKS Statements in the TKS Workbook between meetings.

PT6: Risk Management Strategy (GV.RM-P)
Meeting Schedule

Next Meeting:
Thursday, November 16, 2023
1:00 PM – 2:00 PM EDT

PT6 (GV.RM-P): PrivacyWorkforcePT6+subscribe@list.nist.gov

Project Team 7: Awareness and Training (GV.AT-P)

Co-Leads

Jacqueline Crawley
VP of Governance,
ISACA Atlanta

Ivy Orecchio
Cybersecurity and Privacy Services Manager, Venable LLP

Dr. Elif Kiesow Cortez
Research Fellow,
Stanford Law School

Project Team 7: Awareness and Training (GV.AT-P) Work Assignment

Function: 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.

Privacy Framework Category – Awareness and Training (GV.AT-P): The organization’s workforce and third parties engaged in data processing are provided privacy awareness education and are trained to perform their privacy-related duties and responsibilities consistent with related policies, processes, procedures, and agreements and organizational privacy values.

Subcategory	Description
GV.AT-P1	The workforce is informed and trained on its roles and responsibilities.
GV.AT-P2	Senior executives understand their roles and responsibilities.
GV.AT-P3	Privacy personnel understand their roles and responsibilities.
GV.AT-P4	Third parties (e.g., service providers, customers, partners) understand their roles and responsibilities.

Project Team 7: Awareness and Training (GV.AT-P)

Progress Update

- **Current Status**
  - Leads will review Co-Chairs comments soon
  - Aligned TKS Statements with SP 800-50 [Draft]
- **Goals for this work period**
  - Finalize TKS Statements
  - Ad hoc team meeting if necessary

PT7: Awareness and Training (GV.AT-P)
Meeting Schedule

Next Meeting: **If needed**
Wednesday, November 15, 2023
1:00 PM – 2:00 PM EDT

Project Team 8: Data Processing Management (CT.DM-P)

Abhinav (Abby) Palia,
Sr. Research Scientist,
AWS

Ridwan Badmus,
Legal Associate & CTO,
Oguntoye & Oguntoye LP

Nikita Samarin,
Digital Safety and Privacy
Researcher, UC Berkeley

Project Team 8: Work Assignment

Privacy Framework Function: CONTROL-P (CT-P): Develop and implement appropriate activities to enable organizations or individuals to manage data with sufficient granularity to manage privacy risks.

Privacy Framework Category – Data Processing Management (CT.DM-P): Data are managed consistent with the organization's risk strategy to protect individuals' privacy, increase manageability, and enable the implementation of privacy principles (e.g., individual participation, data quality, data minimization).

Subcategory	**Description**
CT.DM-P1	Data elements can be accessed for review.
CT.DM-P2	Data elements can be accessed for transmission or disclosure.
CT.DM-P3	Data elements can be accessed for alteration.
CT.DM-P4	Data elements can be accessed for deletion.
CT.DM-P5	Data are destroyed according to policy.
CT.DM-P6	Data are transmitted using standardized formats.
CT.DM-P7	Mechanisms for transmitting processing permissions and related data values with data elements are established and in place.
CT.DM-P8	Audit/log records are determined, documented, implemented, and reviewed in accordance with policy and incorporating the principle of data minimization.
CT.DM-P9	Technical measures implemented to manage data processing are tested and assessed.
CT.DM-P10	Stakeholder privacy preferences are included in algorithmic design objectives and outputs are evaluated against these preferences.

Project Team 8: Data Processing Management (CT.DM-P)
Progress Update

- **Current Status**
  - PT8 plans to leverage work done for CT.DM-P1 in the subsequent Subcategories CT.DM-P2 through CT.DM-P4.
  - Completed review of TKS statements for CT.DM-P5 and CT.DM-P6 and sent to PWWG Co-Chairs for review.

- **Goals for this work period:**
  - PT8 will continue reviewing TKS Statements for CT.DM-P7 .

The Co-Leads encourage all members to continue to leave comments on the TKS Statements in the TKS Workbook between meetings.

PT8: Data Processing Management (CT.DM-P)
Meeting Schedule

Next Meeting:
Thursday, November 9, 2023
11:00 AM – 12:00 PM EDT

PT8 (CT.DM-P): PrivacyWorkforcePT8+subscribe@list.nist.gov

Privacy Workforce Working Group
Project Team 9 (PT9)

Data Processing Awareness (CM.AW-P)

Kick off Meeting #1 | November 15, 2023

Team Co-Leads

Stuart Lee
Chief Privacy Officer,
VMware, Inc

Paul Lanois
Partner, Fieldfisher

Shoshana Rosenberg
Founder and General Counsel,
SafePorter

Meeting #2: TBD

Project Team 9: Scope of Work
Data Processing Awareness (CM.AW-P)

Privacy Framework Function: 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.

Privacy Framework Category – Data Processing Awareness (CM.AW-P):Individuals and organizations have reliable knowledge about data processing practices and associated privacy risks, and effective mechanisms are used and maintained to increase predictability consistent with the organization’s risk strategy to protect individuals’ privacy.

Subcategory	Description
CM.AW-P1	Mechanisms (e.g., notices, internal or public reports) for communicating data processing purposes, practices, associated privacy risks, and options for enabling individuals’ data processing preferences and requests are established and in place.
CM.AW-P2	Mechanisms for obtaining feedback from individuals (e.g., surveys or focus groups) about data processing and associated privacy risks are established and in place.
CM.AW-P3	System/product/service design enables data processing visibility.
CM.AW-P4	Records of data disclosures and sharing are maintained and can be accessed for review or transmission/disclosure.
CM.AW-P5	Data corrections or deletions can be communicated to individuals or organizations (e.g., data sources) in the data processing ecosystem.
CM.AW-P6	Data provenance and lineage are maintained and can be accessed for review or transmission/disclosure.
CM.AW-P7	Impacted individuals and organizations are notified about a privacy breach or event.
CM.AW-P8	Individuals are provided with mitigation mechanisms (e.g., credit monitoring, consent withdrawal, data alteration or deletion) to address impacts of problematic data actions.

Q&A

NEXT STEPS

Next Steps
Upcoming Meetings

Project Team 6: Risk Management Strategy (GV.RM-P)
Next Meeting: **Thursday, November 16| 1:00 p.m. – 2:00 p.m. ET**

Project Team 7: Awareness and Training (GV.AT-P)
Next Meeting: **As needed**

Project Team 8: Data Processing Management (CT.DM-P)
Next Meeting: **Thursday, November 9, 2023 |11:00 a.m. - 12:00 p.m. ET**

Project Team 9: Data Processing Awareness (CM.AW-P)
Kickoff Meeting: **Wednesday, November 15, 2023 |2:00 p.m. - 3:00 p.m. ET**

NIST Privacy Workforce Public Working Group
Wednesday, December 13, 2023 |1:00pm – 2:00pm ET

* For updated meeting schedules see the Privacy Workforce Public Working Group | NIST web page.

Next Steps
Mailing List Sign-up

- Privacy Workforce Working Group (PWWG): PrivacyWorkforceWG+subscribe@list.nist.gov

- PT6 (GV.RM-P): PrivacyWorkforcePT6+subscribe@list.nist.gov
- PT7 (GV.AT-P): PrivacyWorkforcePT7+subscribe@list.nist.gov
- PT8 (CT.DM-P): PrivacyWorkforcePT8+subscribe@list.nist.gov
- PT9 (CM.AW-P): PrivacyWorkforcePT9+subscribe@list.nist.gov

- **All mailing lists are moderated**

Next Steps

Troubleshooting

- Email questions to pwwg@nist.gov