NIST Privacy Workforce Public Working Group

Meeting #26
Wednesday, August 9, 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,
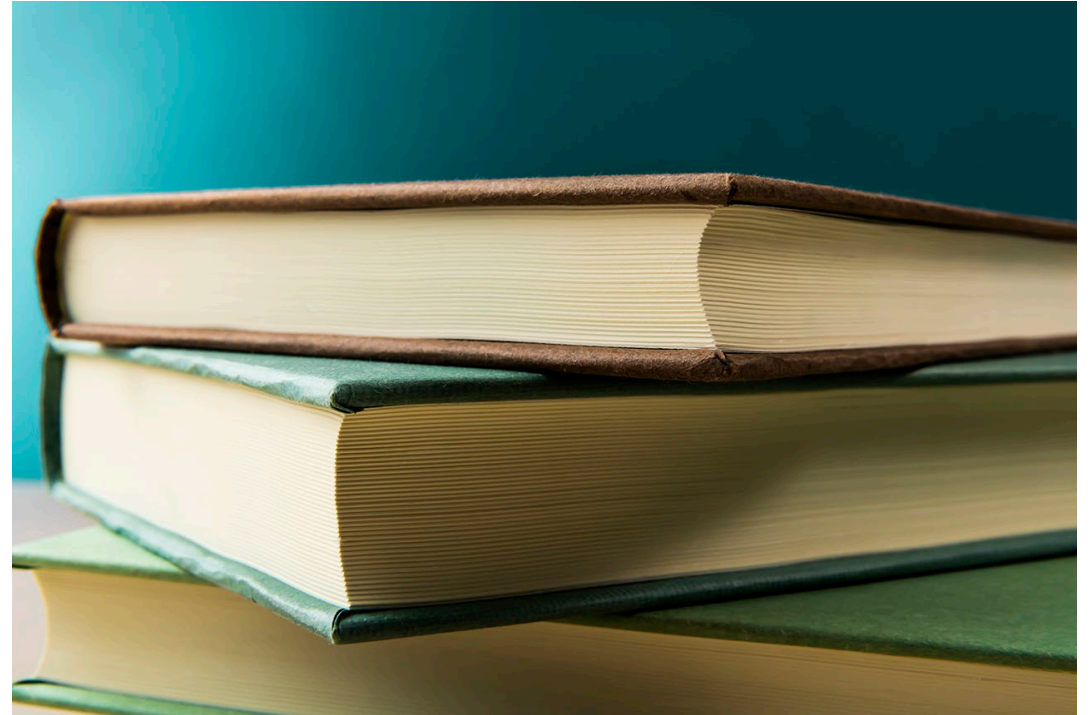PLLC*

Melanie Ensign
Founder & CEO
Discernable, Inc

PWWG UPDATES

PWWG Updates
TKS Compilation Documents

TKS Compilation Inventory

TKS Compilation Mapping

PWWG Updates
TKS Compilation Documents - 2

247 TASK STATEMENTS

253 KNOWLEDGE STATEMENTS

223 SKILL STATEMENTS

PWWG Updates
TKS Standardization -3

- Line edits for syntax and Authoring Guide conformity

- Leverage NICE "Style Guide" for further standardization

- Generate PWWG-specific rules

How should TKS Statements generally refer to stakeholders?

[organization-defined stakeholders]

PWWG Updates
TKS Standardization - 2

Example "Stakeholder" Statements:

Finalize privacy policies with approval from [organization-defined stakeholders].

Identify third-party stakeholder roles and responsibilities to support privacy policies/processes/procedures.

How can we avoid multiple TKS Statements for common phrases in the PF (e.g., policies, processes, and procedures)?

Group commonly occurring phrases together with slashes.

Example "Combined" Statements:

Knowledge of how system/product/service inventories are organized.

Knowledge of existing policies/processes/procedures.

How can we streamline statements that contain assumed knowledge or activities?

Address assumed knowledge and activities within the taxonomy at a location TBD

Example Old "Assumed Knowledge" Statement:

Establish organizational roles, where necessary and feasible, to support third-party stakeholder privacy risk management responsibilities.

Example Updated "Assumed Knowledge" Statement:

Establish a role(s) to support third-party stakeholder privacy risk management responsibilities.

Example Retained "Organization Specific" Statement:

Knowledge of the organization's contract management practices (e.g., storage, location, responsible entity).

Example Old "Assumed Activity" Statements:

Document organizational privacy values.

Maintain documentation of organizational privacy values.

Example Updated "Assumed Activity" Statement:
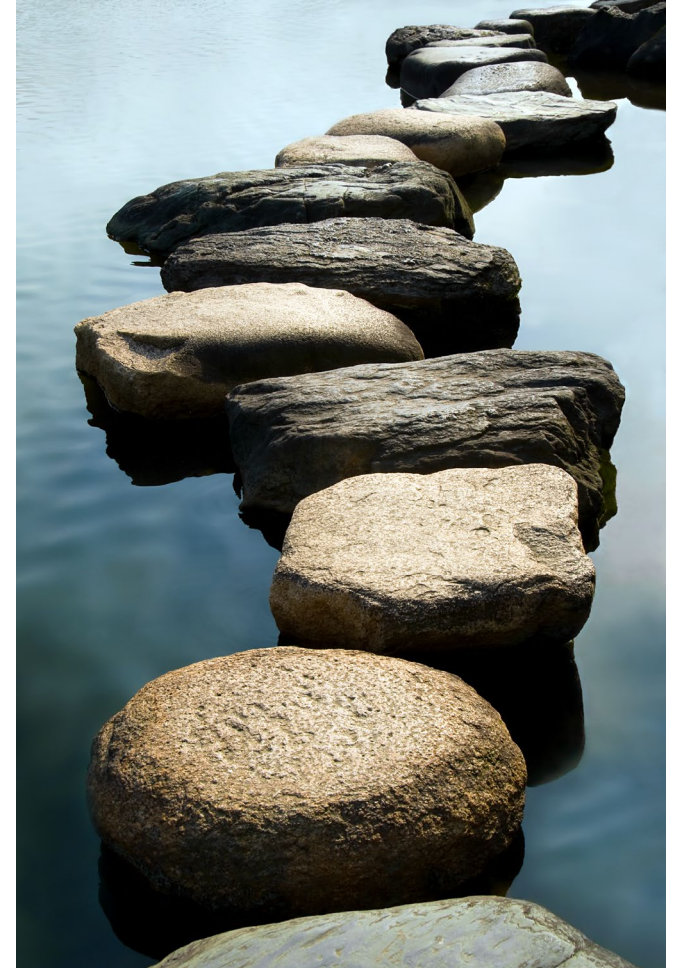
Document organizational privacy values.

PWWG Updates
TKS Standardization: Next Steps

Complete exercise by September monthly call

Include ID.RA-P2 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**
  - Nearing completion of TKS Statements for: **GV.RM-P1**: Risk management processes are established, managed, and agreed to by organizational stakeholders.

- **Goals for this work period:**
  - Continue pre-drafting TKS statements for GV.RM-P2-P3 (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, August 10, 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**
  - Completed Task and Knowledge Statements for :
    GV.AT-P1: The workforce is informed and trained on its roles and responsibilities.

- **Goals for this work period:**
  - Complete Skill Statements for GV.AT-P1.
  - Continue pre-drafting TKS statements for GV.AT-P2 through GV.AT-P4 (Co-Leads).

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

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

Third Meeting:
**Wednesday, August 16, 2023
1:00 PM – 2:00 PM EDT**

PT7 (GV.AT-P): PrivacyWorkforcePT7+subscribe@list.nist.gov
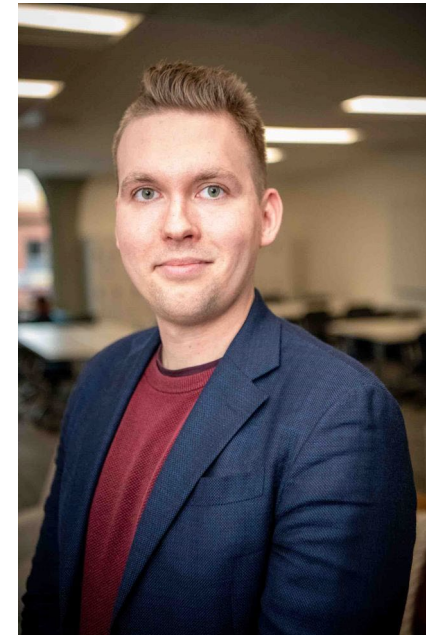
Project Team 8: Data Processing Management (CT.DM-P)

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**
  - Currently working on TKS statements for :
    CT.DM-P1: Data elements can be accessed for review.

- **Goals for this work period:**
  - Complete CT.DM-P1 and send to PWWG Co-Chairs for review.
  - Continue pre-drafting TKS statements for CT.DM-P2 through CT.DM-P10 (Co-Leads).

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

Third Meeting:
**Thursday, August 17, 2023
11:00 AM – 12:00 PM EDT**

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

Q&A

NEXT STEPS

Next Steps
Upcoming Meetings

Project Team 6: Risk Management Strategy (GV.RM-P)
 Next Meeting: **Thursday, August 10| 1:00 p.m. – 2:00 p.m. ET**

Project Team 7: Awareness and Training (GV.AT-P)
 Next Meeting: **Wednesday, August 16, 2023 | 1:00 p.m. – 2:00 p.m. ET**

Project Team 8: Data Processing Management (CT.DM-P)
 Next Meeting: **Thursday, August 17, 2023 |12:00 p.m. - 1:00 p.m. ET**

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

* For updated meeting schedules see the <u>Privacy Workforce Public Working Group | NIST</u> 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

- **All mailing lists are moderated**

Next Steps
Troubleshooting

- Email questions to pwwg@nist.gov