Supplemental Material for Help Wanted: Growing a Workforce for Managing Privacy Risk

On September 22-24, 2020, the International Association of Privacy Professionals (IAPP) will host the virtual public workshop, *Help Wanted: Growing a Workforce for Managing Privacy Risk*. Participants will be able to share their perspective about challenges, needs, and opportunities for developing a skilled and knowledgeable workforce capable of managing privacy risk. The National Institute of Standards and Technology (NIST) plans to use feedback from this workshop to inform the development of a workforce taxonomy aligned with the NIST Privacy Framework: A Tool for Improving Privacy through Enterprise Risk Management (Privacy Framework) and the National Initiative for Cybersecurity Education (NICE) Workforce Framework for Cybersecurity (NICE Framework).

This supplemental material is intended to support participant engagement in the workshop's working sessions. Working session participants are encouraged to review this document and attend the workshop's Opening Plenary (10 a.m. – 12:30 p.m. EDT) on September 22. The Opening Plenary will preview the topics to be explored in working sessions and provide "rules of engagement" for participants. Anyone who cannot attend a working session is still encouraged to provide feedback on this effort.

Why is a privacy workforce taxonomy needed?

The seeds for NIST's privacy workforce effort were planted during the Privacy Framework's development. Throughout that process, stakeholders communicated the need for a broader pool of skilled and knowledgeable professionals comprised of both privacy personnel, as well as those who may not be considered to be privacy professionals per se, but whose activities require some understanding of privacy risk. With a workforce capable of managing privacy risk, organizations should be better equipped to achieve desired privacy objectives and protect individuals' privacy while optimizing beneficial uses of data. The creation of a common understanding around privacy workforce activities could help facilitate the coordination and collaboration necessary to support effective privacy risk management practices. It could also be used to develop more consistent academic curriculae and professional training to support organizations' training and recruitment needs.

What will the privacy workforce taxonomy look like?

We believe that aligning the privacy workforce taxonomy with both the Privacy Framework and the NICE Framework will facilitate organizational efforts to build a workforce that can manage both privacy and cybersecurity risks in a coordinated and effective manner. Though the NICE Framework is currently under revision, the latest draft outlines a structure of tasks, knowledge, skills, work roles, and competencies. Within this structure, knowledge and skill statements are building blocks of both competencies and tasks. Competencies describe the learner who needs to perform the work, while tasks are building blocks of work roles, which describe the work being done. Work roles can be comprised of task statements, and competencies can be comprised of knowledge and skills statements. The purpose of this privacy workforce effort is therefore, not to create a new structure for a taxonomy. Instead, NIST needs to understand how to compose statements in order to produce listings of tasks, knowledge, and skills that can be organized in a modular fashion into work roles and competencies to help organizations achieve the NIST Privacy Framework's outcomes and activities and support training and recruitment of a workforce capable of managing privacy risk.

Working Session Structure

Each virtual working session contains identical programmatic content. The facilitated discussions require pre-registration and will be held under the Chatham House Rule, so there will be no attribution permitted. Interactive engagement will be encouraged through a video conferencing platform, including features such as polling and chats.

The working sessions will focus on the foundational step of task statement creation. Tasks can be used as building blocks to create work roles, which may differ across organizations. In addition, tasks inform what knowledge and skills are needed for the workforce. Although some of the existing tasks, skills, and knowledge statements in the NICE Framework may be leveraged for alignment with Privacy Framework Subcategories, there are gaps that need to be addressed. In the working sessions, NIST is seeking input on two objectives:

- **Objective 1:** determine the appropriate framing of task statements and their relationship to work roles, and
- **Objective 2:** identify tasks necessary to execute on the Privacy Framework.

Objective 1: Framing Task Statements

NIST would like to identify some high-level principles to guide the development of task statements. We want your feedback on how to frame task statements, particularly the appropriate level of abstraction (or granularity) for tasks and the relationship of task statements to work roles.

A. Framing Tasks: Level of Abstraction

Table 1 below shows some current task statements from the NICE Framework and how they could be mapped to a Privacy Framework Subcategory. We selected these tasks to provide examples of different levels of abstraction from high-level or broad activities to more detailed or specific activities. We are interested in understanding whether task statements should be at the same level of abstraction or whether there should be a range. We welcome considerations about how the level of granularity may affect the ability of organizations to achieve Privacy Framework outcomes, as well as the impact on recruitment, training, and cross-organization coordination.

Table 1: Level of Abstraction Task Samples

NICE Framework Task	Privacy Framework Subcategory
T0068: Develop data standards, policies, and procedures**.**	**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.
T0919: Ensure that the company maintains appropriate privacy and confidentiality notices, consent and authorization forms, and materials	
T0901: Assure that the use of technologies maintains, and does not erode, privacy protections on use, collection and disclosure of personal information.	**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.
T0918: Establish, implement and maintains organization-wide policies and procedures to comply with privacy regulations.	**GV.PO-P5:** Legal, regulatory, and contractual requirements regarding privacy are understood and managed.
T0942: Identify the types of information to be processed, stored, or transmitted by a system.	**ID.IM-P6:** Data elements within the data actions are inventoried.

B. Framing Tasks: Relationship to Work Roles

As noted above, a workforce *capable of managing privacy risk* may comprise both privacy professionals and other professionals (e.g., security, legal, IT) who may also execute tasks that contribute to privacy risk management. For example, consider the NICE Framework task in Table 2 and its potential association with the Data Management Category.

Table 2: Technical Task Sample

NICE Framework Task	Privacy Framework Subcategory
T0146 (role implied): Manage the compilation, cataloging, caching, distribution, and retrieval of data**.**	**CT.DM-P4**: Data elements can be accessed for deletion.

Although no specific role is referenced, T0146 is a task that seems more likely to be executed by an IT role than perhaps a legal or other non-technical role. In contrast, Table 3 provides an example of a task which contains embedded roles and some potential adaptations. We would like to understand which type of framing would be most useful and allow suitable flexibility in role assignment for different types or sizes of organizations.

Table 3: Sample Tasks and Relationship to Coordination and Work Roles

NICE Framework Task	Privacy Framework Subcategory
NICE T0862 (role embedded): Work with legal counsel and management, key departments and committees to ensure the organization has and maintains appropriate privacy and confidentiality consent, authorization forms and information notices and materials reflecting current organization and legal practices and requirements.	**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.
NICE T0862 (adapted example 1: role flexibility): Coordinate with [*organization defined work role(s)*] to ensure the organization has and maintains appropriate privacy and confidentiality consent, authorization forms and information notices and materials reflecting current organization and legal practices and requirements.	
NICE T0862 (adapted example 2: role agnostic): Assure that privacy and confidentiality consent, authorization forms and information notices and materials reflect current organization and legal practices and requirements.	

Objective 2: Creating Tasks

We also want to learn about the tasks organizations need to undertake to achieve Privacy Framework outcomes. Due to time constraints, the working sessions will focus on the selected Privacy Framework Categories and Subcategories in the tables below. We would like to hear what tasks participants believe would be necessary to achieve these Subcategories, including what processes and organizational coordination is involved. Following the workshop, we would welcome feedback on other Categories or Subcategories as well.

Table 4: Privacy Framework Inventory and Mapping Category

Category	Subcategory
Inventory and Mapping (ID.IM-P): Data processing	**ID.IM-P1:** Systems/products/services that process data are inventoried.

by systems, products, or services is understood and informs the management of privacy risk.	**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.

Table 5: Privacy Framework Risk Assessment Category

Category	Subcategory
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.

Table 6: Privacy Framework Governance Policies, Processes, and Procedures Category

Category	Subcategory
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.

Stay Engaged

Regardless of whether you are able to attend the workshop, we want you to be part of the process and contribute to the development of the privacy workforce taxonomy. Please send feedback to privacyframework@nist.gov or engage in a community forum via our public Slack channel. To share feedback via Slack, please request access to our channel.

For more information about the NIST privacy workforce effort, visit: https://www.nist.gov/privacy-framework/workforce-advancement

To receive regular updates on this effort, sign up for the Privacy Framework mailing list: http://list.nist.gov/privacyframework