Help Wanted: Growing a Workforce Capable of Managing Privacy Risk: Summary Report

September 22-24, 2020
Virtual Event

On September 22-24, 2020, the International Association of Privacy Professionals (IAPP) hosted a virtual workshop, *Help Wanted: Growing a Workforce Capable of Managing Privacy Risk*. NIST joined the IAPP to lead working sessions where stakeholders shared their perspective about challenges, needs, and opportunities for developing a skilled and knowledgeable workforce capable of managing privacy risk. NIST will use feedback from the workshop to inform the development of a workforce taxonomy aligned with the NIST Privacy Framework: A Tool for Improving Privacy through Enterprise Risk Management[1] (Privacy Framework) and the National Initiative for Cybersecurity Education (NICE) Workforce Framework for Cybersecurity (NICE Framework).[2]

The workshop attracted a large and diverse audience. The opening and closing plenary sessions were attended by 898 and 492 unique users respectively, and the working sessions were attended by 499 participants. Attendees represented a broad spectrum from the public sector and the private sector, including consulting, consumer technology, energy, financial, non-profit, transportation, law, manufacturing, academia, and standards organizations. Participants represented a mixture of roles, including privacy, security, risk management, and compliance, and a range of positions from the executive level to the technical level. Attendees represented geographic diversity as well, with participants joining from 35 countries from around the world. This diversity and the broad range of job roles and responsibilities represented enhanced the depth and complexity of discussions and was critical to the overall success of the workshop.

Workshop Format

Participants were welcomed to the workshop by Omer Tene, Vice President and Chief Knowledge Officer at the IAPP and Kevin Stine, Chief, Applied Cybersecurity Division, NIST.[3] Following the opening remarks, participants heard from three panels that laid the foundation for the working sessions:

- Privacy Risk Management Workforce: The Big Picture
- Building a Workforce Capable of Managing Privacy Risk
- NIST Framework Alignment and Taxonomy Development

The first two panels provided an overview of the challenges organizations face in developing a workforce capable of managing privacy risk and potential ways to meet those challenges. In the final panel, NIST staff gave an update on the revision of the NICE Framework, reviewed the

[1] See https://doi.org/10.6028/NIST.CSWP.01162020.
[2] See https://www.nist.gov/itl/applied-cybersecurity/nice/nice-framework-resource-center.
[3] To view a recording of the opening plenary session, please see https://www.nist.gov/video/webinar-opening-plenary-iapps-help-wanted-growing-workforce-managing-privacy-risk-virtual.

privacy workforce taxonomy development process, and discussed how the two programs are aligning their workforce efforts.

After the opening plenary, participants had the opportunity to participate in facilitated working sessions. Prior to the workshop, NIST had published a supplemental resource intended to guide stakeholder input during the working sessions.[4] As described in the resource, NIST organized the sessions around the foundational step of task statement creation since tasks can be used as building blocks to create work roles, as well as inform what knowledge and skills are needed for the workforce. There were two core objectives:

- Develop principles for how to frame task statements
- Identify activities aligned with the Privacy Framework

The closing plenary session gave participants an opportunity to hear about some of the main takeaways from the working sessions directly from the facilitators.[5] In addition, NIST shared next steps in the taxonomy development process.

General Workshop Themes

During the working sessions, participants engaged in interactive facilitated discussions. The breadth and depth of feedback that NIST received in these sessions reflected the diversity of participating stakeholders. Overall, participants indicated a range of preferences for both the level of task statement abstraction and the extent to which work roles should be embedded or assigned within tasks. Participants signaled that organizations with less developed privacy programs are likely to need more detail and guidance in task statements and role assignments than organizations with more resources and programmatic maturity.

Framing Task Statements

Participants demonstrated a range of preferences for how best to frame task statements. Some participants preferred high-level or more abstract framing of tasks. They found this approach favorable for many reasons, including:

- It gives organizations flexibility to implement or execute tasks in a manner tailored to their programmatic needs.
- Such tasks are more likely to have broad, cross-sector applicability.
- They can provide a useful starting place for organizations to make sure that they aren't missing key tasks.

[4] See https://www.nist.gov/system/files/documents/2020/09/10/Workforce%20Workshop%20Pre-Read%20%289.10.20%29.pdf.

[5] To view a recording of the closing plenary session, please see https://www.nist.gov/video/closing-plenary-iapps-help-wanted-growing-workforce-managing-privacy-risk-virtual-workshop.

Other participants expressed a desire for more granular and discrete task statements framed in specific language. Reasons that they preferred this approach included:

- Conflicting interpretations of task statements can create problems within an organization's workforce or with external vendors who may need to collaborate with the organization to execute the task.
- Such tasks offer more utility than vague and complex or overloaded tasks that can make it time-consuming for organizations to determine how to execute them.
- Organizations with early stage privacy programs may desire or require more guidance when seeking to implement and interpret task statements.

In addition to the appropriate level of abstraction and detail in task statements, the working session discussions also covered other structural framing issues. Participants supported task statements that begin with a strong, active verb to strengthen accountability and minimize confusion around how to execute the task. The discussions also indicated that framing tasks as positive statements can assist with the design and evaluation of performance metrics and goals and can minimize issues with language translation for organizations that work with multi-lingual teams.

Relationship of Tasks to Work Roles

As with task framing, participants provided a range of opinions on the extent to which work roles should be reflected in task statements. Participants were divided between those who preferred tasks that are role agnostic or gave organizations flexibility to assign tasks and those who preferred "clear assignability" of tasks, with a specific role(s) embedded into task statements.

Those who supported task statements without role assignments or statements that gave organizations the ability to choose role assignments found this more flexible approach useful for a variety of reasons, including:

- Responsibilities among workforce roles within an organization (e.g., legal, privacy, and cyber) often overlap.
- Roles, and their related responsibilities, aren't uniform across organizations.
- Organizations with more mature privacy programs can tailor workforce assignments to organization-specific structures and needs.
- There are different ways that a workforce can handle privacy issues and multiple roles can be involved in privacy work.

Reasons that other participants preferred clearly assigned work roles included:

- It helps to make a task actionable.

- Role assignment can assist organizations in identifying who should be responsible for technical tasks.
- Some regulations require organizations to have specific work roles (e.g., the EU General Data Protection Regulation requirement for a Data Protection Officer), and such roles should be clearly defined.
- If no one is responsible for a task, it risks being ignored.
- Smaller organizations or those with less mature privacy programs might not know which role is appropriate or best to assign a task to.
- Clear task assignments support accountability and avoid confusion or workforce "hot potato."

Privacy Framework Alignment Activities

Participants offered substantial feedback on the basic activities that they undertake that align with Category outcomes in the NIST Privacy Framework.[6] The working session discussions focused on describing the general processes that participating organizations have in place to meet the outcomes as well as the different specific steps that are involved in each process. Participants also identified artifacts that they rely on to support these processes. Taken together with the working session discussions around general principles, this feedback provides an excellent starting point for developing the task statements that will form the foundation of the workforce taxonomy.

Next Steps

NIST will consider the body of feedback it received during the workshop and use it to support the development of sets of task, knowledge, and skill statements in alignment with the NICE Workforce Framework for Cybersecurity. These statements can be used in a modular fashion to support achieving Privacy Framework outcomes and activities. Completed resources are anticipated in 2021. NIST continues to encourage additional feedback on the workshop pre-read material. Feedback may be sent to privacyframework@nist.gov.

[6] Due to time constraints, only the following Privacy Framework Categories were discussed: Inventory and Mapping (ID.IM-P), Risk Assessment (ID.RA-P), Governance Policies, Processes, and Procedures (GV.PO-P), Data Processing Ecosystem Risk Management (ID.DE-P), and Data Processing Awareness (CM.AW-P).