Proposed NIST Privacy Framework Roadmap Topic Areas

Note to Reviewers

This document is provided for discussion purposes to promote the development of a companion roadmap to the NIST Privacy Framework: An Enterprise Risk Management Tool (Privacy Framework or Framework). NIST is particularly interested in whether: (i) the proposed topic areas are appropriate for the roadmap; (ii) there are additional areas that should be included; and (iii) the proposed topics appropriately capture priority challenges and gap areas for organizations and key action items to address them. Please send feedback on this document to privacyframework@nist.gov.

Proposed Roadmap Topic Areas

A companion Roadmap to the Privacy Framework will describe plans for advancing the Framework development process, discuss NIST's next steps with the Framework, and identify key areas of development, alignment, and collaboration. It will provide a description of anticipated future activities related to the Framework and offer stakeholders another opportunity to participate actively in the continuing Framework development process.

NIST proposes the following priority areas for inclusion in the Roadmap as they pose challenges to organizations in achieving their privacy objectives. While this list is not intended to be exhaustive, these are important topics identified by stakeholders that should inform future versions of the Privacy Framework. These areas require continued focus as they are important but evolving areas that have yet to be developed or need further research and understanding. While guidance, standards, practices, and tools exist for some of the areas, they need to become more mature, available, and widely adopted. NIST will work with stakeholders to identify primary challenges, solicit input to address those identified needs, and collaboratively develop and execute action plans for addressing challenges.

Mechanisms to Provide Confidence: Mechanisms to provide confidence (e.g., conformity assessment activities, assessments, or audits) can be used to enhance an organization's understanding of its implementation of the Privacy Framework. Effective mechanisms of this type are efficient, transparent, and accessible to organizations regardless of size and resources, drive improvement, and have a sustainable and scalable business case. The lack of mechanisms to provide confidence is a challenge for determining whether organizations are providing effective privacy protections and making good use of limited resources.

Areas of need include research into the organizational challenges and needs with respect to the development of confidence mechanisms, for example, conformity assessment activities, assessment procedures, and externally shared results.

Emerging Technologies: Emerging technologies (e.g., internet of things [IoT], artificial intelligence [AI]) have amplified the complexity of the data processing ecosystem; for example, in IoT, decentralized data processing can involve various third parties that are not contractually bound to any other party, challenging traditional accountability mechanisms. Emerging technologies and the complex data processing ecosystem can add complexity to:

- redress processes,
- individuals' understanding of how their data is processed and how to engage in its processing,
- maintenance of data lineage and provenance, and
- ethical treatment of individuals (e.g., developing AI systems that do not produce biased results, can be explainable, or allow for human intervention capabilities).

Areas of need include research and development to underpin guidance, standards, practices, and related tools for managing privacy risks arising from the use of emerging technologies.

Privacy Risk Assessment: While various privacy risk models have been developed and introduced, organizations continue to face challenges in conducting effective privacy risk assessments.

Areas of need include:

- Uniform concepts of privacy risk factors; and
- More in-depth guidance for assessing privacy risks, including how assessment fits into a risk management approach, and processes for assessing impact to individuals and reflecting that impact within the organization.

Privacy Workforce: Further development of a knowledgeable and skilled privacy workforce (to include privacy practitioners and other personnel whose duties require an understanding of privacy implications) is necessary to support organizations in better protecting individuals' privacy while optimizing beneficial uses of data.

Areas of need include:

- A common lexicon to categorize and describe a privacy workforce, including identification of privacy work roles, the discrete tasks performed by staff within those roles, and the knowledge, skills, and abilities needed to complete the tasks successfully;
- Guidance, standards, practices, and tools to advance the development of a knowledgeable and skilled privacy workforce; and
- Collaboration with organizations that specialize in developing workforce training.

Re-identification Risk: While guidance, standards, practices, and tools are beginning to be developed for de-identification, this area needs to be developed further to promote understanding of how to manage residual re-identification risks.

Areas of need include:

- Increased awareness of re-identification to facilitate identification of these risks (e.g., risks arising from the combination of datasets that were not intended to be combined, magnification of challenge with *emerging technologies*); and
- More guidance, standards, practices, and tools for managing re-identification risks.

Technical Standards: While there are emerging privacy standards in a variety of standards development organizations, to date many of these have been management system standards (focused on processes); there are fewer technical and testing methodology standards in privacy.

Areas of need include:

- Development of standards or adoption of standardized formats for metadata, privacy-enhancing cryptographic techniques, *confidence mechanisms*, and management of *re-identification risk*;
- Additional technical and assessment standards.