Draft NIST Privacy Framework Executive Summary

Note to Reviewers

This document is provided for discussion purposes to promote the development of the NIST Privacy Framework: An Enterprise Risk Management Tool (Privacy Framework). In response to stakeholder feedback received on the Privacy Framework Discussion Draft, released April 30, 2019, NIST has prepared this document to summarize key aspects of the scope and purpose of the Privacy Framework that generated significant dialogue. These themes included privacy risk to individuals and the relationship to organizational risk, privacy risk assessment terminology, the relationship of privacy risk and cybersecurity risk, and organizational roles. This executive summary is more robust than a traditional executive summary by design, to serve as a tool to foster discussion and help NIST understand whether this content better addresses the areas of concern.

NIST is particularly interested in: (i) whether this document fosters a clear understanding of the purpose, value, and scope of the Privacy Framework and (ii) any further gaps or areas for clarification. Please send feedback on this document to privacyframework@nist.gov. NIST will use the feedback to inform the development of a preliminary draft of the Privacy Framework.

Draft NIST Privacy Framework Executive Summary

For more than two decades, the Internet and associated information technologies have driven unprecedented innovation, economic value, and improvement in social services. Many of these benefits are fueled by data about individuals that flow through a complex ecosystem—so complex that individuals may not be able to understand or attend to the potential consequences for privacy resulting from their interactions with systems, products, and services. At the same time, organizations may not realize the full extent of these consequences for individuals, for society, or for their enterprises, which can affect their reputations, their bottom line, and their future prospects for growth.

Approaches to privacy have been challenging because privacy is an all-encompassing concept. It is a condition or state that safeguards important values such as human autonomy and dignity, yet the means for achieving it vary. This broad and shifting nature of privacy makes it difficult to communicate clearly about privacy risks within and between organizations and with individuals.

As part of its mission to further technological innovation and increase trust in information systems, the National Institute of Standards and Technology (NIST), working in collaboration with private and public stakeholders, has developed the voluntary NIST Privacy Framework: An Enterprise Risk Management Tool (Privacy Framework). The Privacy Framework provides a shared lexicon and is a practical tool that can assist organizations—even those fully compliant with relevant laws or regulations—in making ethical decisions when designing or deploying their products and services and avoiding losses of trust that damage their reputations and can slow adoption or cause abandonment of these products and services. It does this by helping organizations consider:

- How their systems, products, and services affect individuals; and
- How to integrate practices into their risk management processes that optimize beneficial uses of data while minimizing adverse effects on individuals' privacy.

Deriving benefits from data while simultaneously managing risks to individuals' privacy is not well-suited to one size-fits-all solutions. The Privacy Framework—through a risk- and outcome-based approach—is flexible enough to address diverse privacy needs and stay current with broader technology trends, including artificial intelligence and the Internet of Things.

The approach of the Privacy Framework is to consider potential problems individuals could experience arising from system, product, or service operations with data, whether in digital or non-digital form, through a complete life cycle, or in other words: from data collection through disposal. The Privacy Framework describes these data operations in the singular as a *data action* and collectively as *data processing*. The problems individuals can experience as a result of data processing can be expressed in various ways, but NIST describes them as ranging from dignity-type losses such as embarrassment, stigmas, or discrimination to more tangible harms such as economic loss or physical harm. These problems can arise from cybersecurity incidents where there is a loss of confidentiality, integrity, or availability at some point in the data processing, including the unauthorized access or use of data by employees who exceed their authorized privileges. However, problems also can arise from data processing that is intentional or "authorized" (whether under law or explicit or implicit organizational policy) that organizations conduct to meet their mission or business objectives.

Once an organization can identify the likelihood of any given problem arising from the data processing, which the Privacy Framework refers to as a *problematic data action*, it can assess the impact should the problematic data action occur. This impact assessment is the intersection between privacy risk and organizational risk. Individuals experience the direct impact of problems, but an organization may experience "secondary" impacts, such as noncompliance costs, customer abandonment of products and services, or harm to its external brand reputation or internal culture. These organizational impacts can be drivers for informed decision-making about resource allocation to strengthen privacy programs and to help organizations bring privacy risk into parity with other risks they are managing at the enterprise level.

Given the overlap with data security, the Privacy Framework can be used in conjunction with the Framework for Improving Critical Infrastructure Cybersecurity (Cybersecurity Framework) to manage the data security aspect of privacy risk. [*Alternate sentence for the Core Version A*: Given the overlap with data security, the Privacy Framework integrates and adapts Core Functions, Categories and Subcategories from the Framework for Improving Critical Infrastructure Cybersecurity (Cybersecurity Framework) to support coordinated management of the data security aspect of privacy risk.] To further facilitate alignment, the Privacy Framework follows the structure of the Cybersecurity Framework and is composed of three parts: the Core, the Profiles, and the Implementation Tiers. Each component reinforces privacy risk management through the connection between business and mission drivers and privacy protection activities.

- The Core enables an organization—from the executive level to the implementation/operations level—to have a dialogue about and prioritize privacy protection activities and desired outcomes. *An organization may not need to achieve every outcome or activity reflected in the Core.*
- An organization uses the process of developing Profiles to prioritize the selection of the outcomes and activities that best meet its specific needs, taking into consideration its organizational or industry sector goals, legal or regulatory requirements and industry best practices, risk management priorities, and the privacy needs of individuals who are directly or indirectly served or affected by the organization's systems, products, or services.

- The Implementation Tiers are meant to support organizational decision-making and communication about how to manage privacy risk by taking into account the nature of the privacy risks engendered by the organization's systems, products, or services and the adequacy of the processes and resources the organization has in place to manage such risks.

The Privacy Framework is intended to be widely usable by organizations of all sizes and agnostic to any particular technology, sector, law, or jurisdiction. Different parts of an organization's workforce, including executives, legal, and IT may take responsibility for different outcomes and activities. Ideally, the Privacy Framework encourages cross-organization collaboration to develop Profiles and achieve outcomes. The Privacy Framework also is intended to be usable by any organization or entity regardless of its role in the *data processing ecosystem*—which comprises the complex and interconnected relationships among entities involved in creating or deploying systems, products, or services or any components that process data. Some laws or industry sectors classify organizational roles—to allow for broad use, the Privacy Framework does not—but an organization should review the outcomes and activities in the Privacy Framework from its standpoint in the ecosystem and consider how to manage privacy risk not only with regard to its internal priorities, but also in relation to how they affect other parties' management of privacy risk.

While privacy is often discussed in compliance terms, the Privacy Framework highlights that regulatory compliance is only one piece of the puzzle, and often should be viewed as the floor instead of the ceiling. A risk-based approach to privacy allows the flexibility for more innovative and effective solutions that can lead to better outcomes for individuals and enterprises. Much work remains: privacy risk management is still a nascent discipline in contrast to cybersecurity risk management. The Privacy Framework is a foundation, but NIST, in collaboration with stakeholders, intends to build a repository of informative references of additional guidance and shared best practices to help organizations achieve the Privacy Framework outcomes and activities and build trust in their systems, products, and services through the protection of individuals' privacy.