NIST Privacy Framework Working Outline

Notes to Reviewers

This document is provided for discussion purposes to promote input on the NIST Privacy Framework: An Enterprise Risk Management Tool (Privacy Framework). NIST does not plan to produce another version of this outline. NIST will use feedback on this outline to develop a discussion draft of the Privacy Framework.[1]

Reading the outline: Plain text indicates preliminary text for the Privacy Framework discussion draft. Alternatively, italicized text describes what content will be included within a section or for commentary about how the content is responsive to what NIST has heard from stakeholders, including responses to the Notice of Request for Information (RFI) released on November 14, 2018.[2,3]

Based on stakeholder feedback, this outline provides a high-level alignment with the Framework for Improving Critical Infrastructure Cybersecurity (Cybersecurity Framework) to enable greater compatibility between the two frameworks. NIST welcomes feedback on this alignment, including the level of alignment desired in the Privacy Framework or the appropriateness of the alignment considering the current guidance needs of the two disciplines.

The RFI responses indicated that there is not a consistent or widespread understanding of privacy risk management, so NIST plans to provide a more in-depth treatment of the subject in an appendix to the Privacy Framework. NIST also included an appendix for a roadmap covering NIST's next steps and identifying key areas for development of best practices for privacy risk management.

At a minimum, NIST would like feedback on whether the organization and content of this outline is a constructive approach for the Privacy Framework. There are many additional details that will be provided in the upcoming discussion draft, such as specific categories and subcategories for the Privacy Framework Core, but NIST also welcomes feedback on what reviewers would like to see included.

Please send feedback on this outline to privacyframework@nist.gov.

[1] See *Development Schedule* at https://www.nist.gov/privacy-framework.

[2] See *Summary Analysis of the Responses to the NIST Privacy Framework Request for Information* at https://www.nist.gov/privacy-framework.

[3] *Developing a Privacy Framework: A Notice by the National Institute of Standards and Technology on 11/14/2018*, https://www.federalregister.gov/documents/2018/11/14/2018-24714/developing-a-privacy-framework.

Table of Contents

Executive Summary

The Executive Summary will provide an overview of the Privacy Framework to facilitate an understanding of its purpose and benefits.

1. Privacy Framework Introduction

RFI respondents overwhelmingly supported a framework that is risk-based, outcome-based, voluntary, and non-prescriptive; adaptable to many different organizations, technologies, lifecycle phases, sectors, and uses; provides a common and accessible language; and is compatible with and supports organizations' ability to use global standards and operate under applicable domestic and international legal or regulatory regimes. This introductory section will describe how the Privacy Framework is designed and structured to achieve these attributes.

Although the Privacy Framework is aligned with the structure of the Cybersecurity Framework to assist organizations that want to use both frameworks, good cybersecurity practices alone are not sufficient to address the full scope of privacy risks that can arise from how organizations collect, store, use, and disclose data (collectively "data processing") to meet their mission or business objectives, as well as from how individuals interact with products, services, or systems. Consequently, this section will clarify the relationship and the differences between the cybersecurity and privacy disciplines to establish the reasoning behind the privacy-specific adaptations NIST has made for the Privacy Framework.

In addition, this section will provide an overview of privacy risk management as a process that supports organizations' optimization of beneficial uses of data while minimizing the potential for *adverse effects on individuals. Notwithstanding this overview, the RFI responses indicated that there is not a consistent or widespread understanding of privacy risk management. For example, many RFI responses acknowledged the lack of widely-agreed upon concepts that are essential to privacy risk management such as a uniform privacy risk model. To address this gap, NIST will provide a more in-depth treatment of privacy risk management in Appendix D.*

2. Privacy Framework Basics

Following the structure of the Cybersecurity Framework, this section will describe the three components of the Privacy Framework: the Core, Profiles, and Tiers. In addition to the use of the Cybersecurity Framework structure, many RFI respondents expressed support for other organizational constructs such as the information life cycle, privacy principles, and the NIST privacy engineering objectives.[4] *These constructs will be reflected in the elements of the Core as well.*

2.1. Privacy Framework Core

The Privacy Framework Core (Core) will provide a set of activities to achieve specific privacy outcomes, and reference examples of guidance to achieve those outcomes. The Core is not a checklist of actions to perform. It will present key privacy outcomes identified by stakeholders as helpful in managing privacy risk. The Core will comprise four elements: functions, categories, subcategories, and informative references, depicted in ***Figure 1****:*

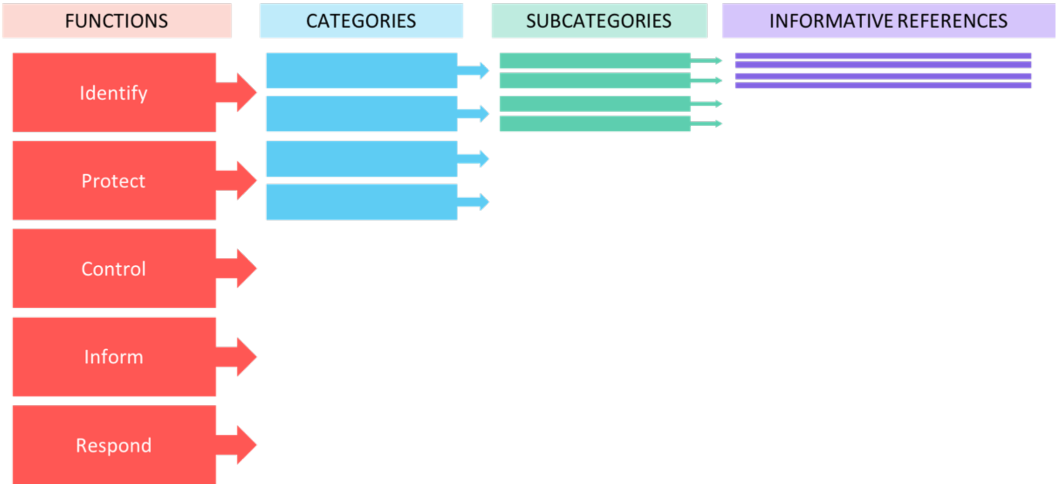

Figure 1: Privacy Framework Core Structure

The functions organize basic privacy activities related to data processing at their highest level. The functions will be divided into categories closely tied to programmatic needs and subcategories to support specific outcomes for organizations' technical or management

[4] *NIST Internal Report 8062: Introduction to Privacy Engineering and Risk Management in Federal System*, at 17, https://nvlpubs.nist.gov/nistpubs/ir/2017/NIST.IR.8062.pdf.

activities. Informative references will provide organizations with guidance in achieving the outcomes.

The functions are:

- **Identify** – Develop the organizational understanding to manage privacy risk for individuals arising from data processing or their interactions with products, services, or systems.

  The activities in the Identify function will be foundational for effective use of the Privacy Framework. Understanding the business context, including the circumstances under which data is processed, the privacy interests of individuals directly or indirectly served by the organization, and legal/regulatory requirements will enable an organization to focus and prioritize its efforts, consistent with its risk management strategy and business needs. The categories and subcategories will be adapted from the Cybersecurity Framework Identify function to support privacy risk management practices, and additional categories and subcategories may be included based on stakeholder input. Examples of outcome categories within this function may include: Asset Management; Business Environment; Governance; Risk Assessment; and Risk Management Strategy.

- **Protect** – Develop and implement appropriate data safeguards.

  The Protect function encapsulates the overlap between privacy and cybersecurity around data security and will also include practices aligned with the disassociability privacy engineering objective. Many of the categories and subcategories may be cross-referenced from the Cybersecurity Framework. In addition, a number of RFI respondents encouraged NIST to include practices around de-identification and privacy-enhancing cryptography. Examples of outcome categories within this function may include: Identity Management and Access Control; Awareness and Training; Data Security; and De-identification.

- **Control** - Develop and implement appropriate activities to enable organizations or individuals to manage data with sufficient granularity to meet privacy objectives.

  The Control function considers data management from both the standpoint of the organization and the individual. A number of RFI responses acknowledged this dual concept of control. This function aligns with the manageability privacy engineering objective which emphasizes the value of engineering this capability into systems and products in order to achieve important privacy principles such as accountability, data minimization, data access (including correction and deletion), individual participation, and others. Examples of outcome categories within this function may include: Data Management, Data Quality, Default Configurations, and User Preferences.

- **Inform** - Develop and implement appropriate activities to enable organizations and individuals to have a reliable understanding about how data is processed.

  The Inform function recognizes that both organizations and individuals need to know how data is processed in order to manage privacy risk effectively. This function aligns with *the predictability privacy engineering objective and supports the key privacy principle of transparency. A number of RFI responses emphasized the importance of this principle in both current and emerging technologies. Examples of outcome categories within this function may include: User Notices, Data Processing Reporting, and Algorithmic Transparency.*

- **Respond** – Develop and implement appropriate activities to take action regarding a privacy breach.

  The Respond function supports the ability to provide redress for individuals who have experienced a privacy breach. Categories and subcategories may be cross-referenced from the Cybersecurity Framework, and additional categories and subcategories may be included based on stakeholder input. Examples of outcome categories within this function may include: Redress and Breach Notification.

2.2. Privacy Framework Profile

The Privacy Framework Profile ("Profile") is the alignment of the functions, categories, and subcategories with the business requirements, risk tolerance, privacy objectives, and resources of the organization. Under the risk-based approach of the Privacy Framework, organizations may not need to achieve every outcome or activity reflected in the Core. Thus, when developing a Profile, an organization may select or tailor the functions, categories, and subcategories of the Privacy Framework to its specific organizational needs. Organizations determine these needs through consideration of organizational or industry sector goals, legal/regulatory requirements and industry best practices, the privacy needs of individuals who are part of—or directly or indirectly served by—an organization, and the organization's risk management priorities. A current Profile indicates privacy outcomes that an organization is currently achieving, while a target Profile indicates the outcomes needed to achieve the desired privacy risk management goals. The differences between the two Profiles enables an organization to gauge the resources that would be needed (e.g., staffing, funding) to achieve privacy goals and forms the basis of an organization's plan for reducing privacy risk in a cost-effective, prioritized manner. Profiles also can aid in communicating risk within and between organizations by helping organizations understand and compare the current or desired state of privacy outcomes.

2.3. Privacy Framework Implementation Tiers

The Privacy Framework Implementation Tiers ("Tiers") provide context on how an organization views privacy risk and the processes in place to manage that risk. Aligned with the Cybersecurity Framework, there are four distinct tiers: Partial (Tier 1), Risk Informed (Tier 2), Repeatable (Tier 3), and Adaptive (Tier 4). Tiers do not represent maturity levels. While organizations identified as Tier 1 are encouraged to consider moving toward Tier 2, Tiers are meant to support organizational decision making about how to manage privacy risk by taking into account the nature of the privacy risks engendered by the organization's products, services, or systems and the cost and effectiveness of the risk management practice. Thus, some organizations may never need to achieve Tier 3 or 4 or may only focus on certain areas of these tiers. Progression to higher Tiers is necessitated when the nature of the privacy risks requires more multi-faceted risk management practices. Successful implementation of the Privacy

Framework is based upon achieving the outcomes described in the organization's Target Profile(s) and not upon Tier determination.

The Tiers are defined through four areas summarized below. The first two areas are consistent with the Cybersecurity Framework. NIST has adapted the third area to focus more explicitly on ecosystem relationships and the role that all entities (e.g., consumer-facing organizations, service providers, product manufacturers, software developers) play in managing privacy risks for individuals. NIST has added a fourth area for workforce based on the RFI responses recognizing that privacy workforce development is a critical need. Although coordination among various organizations, including academic institutions and training certification organizations, will be necessary to achieve a skilled privacy workforce, organizations using the Privacy Framework can support this coordination by communicating their privacy risk management needs and providing demand for the desired skillsets.

- Privacy Risk Management Process: *Ranging from informal, ad hoc privacy risk management processes at Tier 1 to processes that enable continuous adaptation to changing technologies and data processing activities, and incorporate the use of advanced privacy-enhancing technologies and practices, at Tier 4.*

- Integrated Privacy Risk Management Program: *Ranging from a limited awareness of privacy risk at the organizational level at Tier 1 to all levels of the organization being able to make decisions with a clear understanding of the relationship between privacy risk, other types of risk (including cybersecurity risk), and organizational objectives at Tier 4.*

- Ecosystem Relationships: *Ranging from the entity does not understand its role in the larger ecosystem with respect to other entities (e.g. buyers, suppliers, service providers, business associates or partners, product or service end-users, regulators) at Tier 1 to the entity understands its role in the larger ecosystem and contributes to the community's broader understanding and management of privacy risks at Tier 4.*

- Workforce: *Ranging from a workforce that has little or no understanding of privacy risks at Tier 1 to a workforce that includes specialized privacy skillsets throughout the organizational structure at Tier 4.*

3. How to Use the Privacy Framework

This section covers how organizations can use the Privacy Framework to establish or improve their privacy risk management practices and communicate them throughout the organization. As noted by a number of RFI respondents, it will emphasize the importance of integrating privacy risk management throughout the entire life cycle of data processing, from collection through disposal. It will provide simple steps for using the Privacy Framework as part of an organization's broader risk management approach, including in conjunction with other risk management frameworks that an organization may be using such as the Cybersecurity Framework or the Risk Management Framework for Information Systems and Organizations: A

System Life Cycle Approach for Security and Privacy.[5] *The Privacy Framework provides a common language to communicate privacy requirements. Thus, this section also will include examples of how organizations can use various components of the Privacy Framework to discuss privacy requirements with different stakeholders, and inform decisions about buying products and services—along with how to track and address residual privacy risk once a product or service is purchased.*

Appendix A: Privacy Framework Core

This table will be completed with categories, subcategories, and informative references.

Functions	Categories	Subcategories	Informative References
Identify			
Protect			
Control			
Inform			
Respond			

Appendix B: Glossary

This appendix defines selected terms used in the publication to aid organizations in the use of the Privacy Framework. This section is not intended to define general usage privacy terms.

Appendix C: Acronyms

This appendix defines selected acronyms used in the publication.

[5] *NIST SP 800-37 Rev. 2, Risk Management Framework for Information Systems and Organizations: A System Life Cycle Approach for Security and Privacy*, https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-37r2.pdf.

Appendix D: Privacy Risk Management

This appendix offers a more in-depth discussion of privacy risk management to provide organizations that do not yet have robust processes with considerations on how to assess and prioritize privacy risks, and make considered decisions on how to respond to them through the integration of privacy engineering objectives, privacy principles, and legal/regulatory requirements into the business environment and system or product development and operations.

Appendix E: Roadmap

This appendix will provide a companion roadmap to the Privacy Framework covering NIST's next steps and identifying key areas for development of best practices for privacy risk management. These areas will be based on input and feedback received from stakeholders through the Privacy Framework development process about outcomes that lack sufficient informative references or the relevant practices are not well enough understood to enable organizations to achieve the outcome.