Comment Template for Privacy Framework 1.1 Initial Public Draft

Please submit responses to: privacyframework@nist.gov by ***June 13, 2025***

NAME: Matthew Reisman
ORGANIZATION: Centre for Information Policy Leadership
EMAIL: mreisman@hunton.com

Line #	Page #	Section	Proposed Change	Comment (Include rationale for proposed change(s))
				General comment : The Centre for Information Policy Leadership (CIPL) welcomes the opportunity to comment on the NIST Privacy Framework 1.1 Initial Public Draft. CIPL is a global privacy and data policy think tank within the Hunton law firm that is financially supported by the firm, 85+ member companies that are leaders in key sectors of the global economy, and other private and public sector stakeholders through consulting and advisory projects. CIPL's mission is to en in thought leadership and develop best practices for the responsible and beneficial use of data in the modern information age. CIPL's work facilitates construct engagement between business leaders, data governance and security professionals, regulators, and policymakers around the world. For more information, ple see CIPL's website at www.informationpolicycentre.com. Nothing in this document should be construed as representing the views of any individual CIPL memb company or Hunton. This document is not designed to be and should not be taken as legal advice.
				General comment: CIPL appreciates NIST's efforts to modernize the NIST Privacy Framework in recognition of recent technological developments and to updat in a manner that preserves interoperability with the recently updated NIST Cybersecurity Framework - both of which will ensure the Framework remains maxi relevant and useful for practitioners.
				General Comment: NIST asked in the consultation document: "Should NIST re-number Unique Identifiers in the Privacy Framework 1.1 Final Draft to avoid gap numbering?" CIPL recommends that NIST retain the gaps in numbering and not re-number the unique identifiers so as to avoid creating backward compatibilit issues for organizations that have built governance processes consistent with the numberings in the Privacy Framework 1.0.
				General Comment: NIST asked in the consultation document: "Should NIST further streamline the Privacy Framework 1.1 PDF by removing content from the PD (e.g., Appendices) and relocating it?" CIPL agrees that this would be helpful. Doing so would enable the information to more readily be kept up to date and facilitate interactive use by organizations seeking to implement the Framework.
				General Comment: NIST asked in the consultation document: "Should NIST include Privacy Framework 1.1 Implementation Examples as supplemental materia the PF 1.1 Final Draft? If so, would a mapping of Task Statements from the NIST Privacy Workforce Taxonomy to the Privacy Framework 1.1 Core be a useful approach to creating Implementation Examples?" CIPL agrees that implementation examples would be helpful. CIPL has found that practical case studies are valuable for helping organizations determine how to implement accountable data governance. Aligning the examples with the NIST Privacy Workforce Taxono would be a useful approach.
246-303	pages 5-6	1.1.1		Section 1.1.1 includes a clear and helpful conceptual crosswalk between cybersecurity and privacy risk management (pages 5-6).
306-353	pages 7-8	1.2.2	Add the language in brackets to the following sentence (which starts on line 342): *For example, differentially private synthetic data could be used to train machine learning models while enhancing the privacy protections for the original data. Yet, the synthetic generation process may skew distributions and introduce other biases, which can propagate to downstream applications,* ***[if not implemented with careful attention to preventing or mitigating such potential effects]*** .	The addition to the Framework of a section on AI and Privacy Risk Management (1.2.2) is valuable. CIPL has produced numerous works examining this relations in detail (please see www.informationpolicycentre.com for links to our publications, which can be accessed and downloaded free of charge). We suggest that devote additional attention within the framework to the unique considerations that generative AI may pose for privacy principles, and how those principles ca interpreted in a manner that respects individuals' privacy while enabling innovation and enjoyment of the benefits of generative AI. Please see our discussion paper on *Applying Data Protection Principles to Generative AI: Practical Approaches for Organizations and Regulators* (December 2024) for additional details. V respect to our suggested change to the sentence about the use of synthetic data (displayed in the column to the left), please find more information in our whit paper on *Privacy-Enhancing and Privacy-Preserving Technologies in AI: Enabling Data Use and Operationalizing Privacy by Design and Default* (March 2025).
354-394	pages 8-10	1.2.3		The discussion of risk assessment on pages 8-10 usefully distinguishes privacy risks to individuals vs. risks to organizations, and compliance risks vs. risks to organizational trust/reputation. CIPL has written about data governance frameworks centered on concepts of organizational accountability that are broadly consistent with these and other concepts in the NIST Framework; our reports may be useful points of reference for organizations seeking examples and practic tools for building their own governance programs. Please see *Building Accountable AI Programs: Mapping Emerging Best Practices to the CIPL Accountability Framework* February 2024) and *What Good and Effective Data Privacy Accountability Looks Like: Mapping Organizations' Practices to the CIPL Accountability Framework* (May 2020).
471-473	page 12	2.1	Add language acknowledging that many activities related to "Protect-P" functions, such as incident response, may be led by a single team or internal teams working closely together.	Integration of data governance functions, including privacy and cybersecurity, is happening in organizations that are seeking to build a more holistic approach data strategy and governance. It is important for the Privacy Framework to acknowledge this reality and avoid the implication that organizations must create parallel processes in instances where they would be redundant or less effective. For more information, see CIPL,*Leveraging Data Responsibly: Why Boards and C-Suite Need to Embrace a Holistic Data Strategy* , April 2024.