Draft NIST Privacy Framework Glossary (Updated)

Attribute Reference [NIST SP 800-63-3]	A statement asserting a property of a subscriber without necessarily containing identity information, independent of format. For example, for the attribute "birthday," a reference could be "older than 18" or "born in December."
Attribute Value [NIST SP 800-63-3]	A complete statement asserting a property of a subscriber, independent of format. For example, for the attribute "birthday," a value could be "12/1/1980" or "December 1, 1980."
Availability [NIST SP 800-37]	Ensuring timely and reliable access to and use of information.
Category	The subdivision of a function into groups of privacy outcomes, closely tied to programmatic needs and particular activities. Examples of categories include "Data Management," "Inventory and Mapping," and "Risk Assessment."
Communicate (Function)	Develop and implement appropriate activities to enable organizations and individuals to have a reliable understanding about how data are processed and associated privacy risks.
Confidentiality [NIST SP 800-37]	Preserving authorized restrictions on information access and disclosure, including means for protecting personal privacy and proprietary information.
Control (Function)	Develop and implement appropriate activities to enable organizations or individuals to manage data with sufficient granularity to manage privacy risks.
Core	A set of privacy protection activities, desired outcomes, and applicable references. The Framework Core comprises three types of elements: functions, categories, and subcategories.
Data	A representation of information, including digital and non-digital formats, with the potential for adverse consequences for individuals when processed.
Data Action [NISTIR 8062, Adapted]	A system/product/service operation that processes data.
Data Element	The smallest named item of data that conveys meaningful information.
Data Processing [NISTIR 8062, Adapted]	An operation or set of operations performed upon data across the full data life cycle, including but not limited to collection, retention, logging, generation, transformation, use, disclosure, transfer, and disposal.
Data Processing Ecosystem	The complex and interconnected relationships among entities involved in creating or deploying systems, products, or services or any components that process data.

Disassociability [NISTIR 8062, Adapted]	Enabling the processing of data or events without association to individuals or devices beyond the operational requirements of the system.
Function	One of the main components of the Privacy Framework. Functions provide the highest level of structure for organizing basic privacy activities into categories and subcategories. The six functions are Identify, Govern, Protect, Communicate, Control, and Respond. [Alternate for Core Version B: The four functions are Identify, Govern, Communicate, and Control.]
Govern-P (Function)	Develop and implement the organizational governance structure to enable an ongoing understanding of the organization's risk management priorities that are informed by privacy risk.
Identify-P (Function)	Develop the organizational understanding to manage privacy risk for individuals arising from system, product, or service data processing.
Implementation Tier	The degree to which an organization's current or target risk management practices demonstrate an understanding of privacy risk and how systematic the practices are.
Integrity [NIST SP 800-37]	Guarding against improper information modification or destruction, and includes ensuring information non-repudiation and authenticity.
Lineage	The history of processing of a data element, which may include point to point data flows and the data actions performed upon the data element.
Manageability [NISTIR 8062, Adapted]	Providing the capability for granular administration of data, including alteration, deletion, and selective disclosure.
Metadata [NIST SP 800-53, Adapted]	Information describing the characteristics of data including, for example, structural metadata describing data structures (i.e., data format, syntax, semantics) and descriptive metadata describing data contents.
Predictability [NISTIR 8062, Adapted]	Enabling reliable assumptions by individuals, owners, and operators about data and its processing by a system, product, or service.
Privacy Breach	The loss of control, compromise, unauthorized disclosure, unauthorized acquisition, or any similar occurrence where (1) a person other than an authorized user accesses or potentially accesses data or (2) an authorized user accesses data for an other than authorized purpose.
Privacy Control [NIST SP 800-37, Adapted]	The administrative, technical, and physical safeguards employed within an organization to satisfy privacy requirements.
Privacy Event	The occurrence of problematic data actions.
Privacy Requirement	A specification for system/product/service functionality to meet stakeholders' desired privacy outcomes.

Privacy Risk	The likelihood that individuals will experience problems resulting from data processing, and the impact should they occur.
Privacy Risk Assessment	A privacy risk management sub-process for identifying, evaluating, prioritizing, and responding to specific risks arising from data processing.
Privacy Risk Management	A cross-organizational set of processes for identifying, assessing, and responding to privacy risks.
Problematic Data Action [NISTIR 8062]	A data action that can cause an adverse effect, or problem, for individuals.
Processing	See *Data Processing*
Profile	A representation of the outcomes based on business/mission objectives, types of data processing, and individuals' privacy needs that an organization has selected from the Privacy Framework categories and subcategories.
Protect-P (Function)	Develop and implement appropriate data processing safeguards.
Provenance [NISTIR 8112, Adapted]	Metadata pertaining to the origination or source of specified data.
Respond-P (Function)	Develop and implement appropriate activities to take timely action regarding a privacy breach or event.
Risk [NIST SP 800-30]	A measure of the extent to which an entity is threatened by a potential circumstance or event, and typically a function of: (i) the adverse impacts that would arise if the circumstance or event occurs; and (ii) the likelihood of occurrence.
Subcategory	The further divisions of a category into specific outcomes of technical and/or management activities. Examples of subcategories include "Systems/products/services that process data are inventoried," "Data are processed to limit the identification of individuals," and "Data corrections or deletions can be communicated to individuals or organizations (e.g., data sources)."