

1 Proposed Separated Core

2 *Proposed Version of the NIST Privacy Framework Core without Data Security*

3 Note to Reviewers

4 This Separated Core is provided for discussion purposes to promote the development of the NIST Privacy
5 Framework: An Enterprise Risk Management Tool (Privacy Framework). In response to stakeholder
6 feedback received on the Privacy Framework Discussion Draft (Discussion Draft), released April 30, 2019,
7 NIST has prepared two different, updated versions of the Core for feedback.

8 The two proposed Cores offer different levels of alignment with the Framework for Improving Critical
9 Infrastructure Cybersecurity (Cybersecurity Framework). For this Separated Core, NIST has removed the
10 overlapping Cybersecurity Framework Functions, Categories, Subcategories that pertain to data security.
11 Organizations that want to manage the data security aspect of privacy risk should use the Cybersecurity
12 Framework Core. In contrast, for the Integrated Core, NIST has maintained a number of data security
13 Functions, Categories, and Subcategories that overlap with the Cybersecurity Framework.

14 In addition, each Core contains the same updates based on specific feedback on the Discussion Draft
15 Core. See below for a summary of material changes.

16 NIST is particularly interested in feedback on: (i) which proposed Core is preferred by stakeholders, (ii)
17 why that proposed Core is preferred; and (iii) any additional changes to either of the proposed Cores to
18 support organizations' needs with respect to managing privacy risk.

19 Please send feedback on the proposed Core versions to privacyframework@nist.gov. NIST will use
20 feedback on this document to inform the development of a preliminary draft of the Privacy Framework.

21 Summary of Material Changes from the Discussion Draft Core

22 The Separated Core retains three of the five Functions presented in the Discussion Draft (*Identify*,
23 *Control*, and *Communicate*), with some modifications: creation of a new Function, *Govern*, that splits off
24 some Categories from *Identify*, and renaming *Inform* to *Communicate*. This version removes the
25 Functions *Protect* and *Respond* that support the data security aspect of privacy risk,. **Figure 1** was added
26 to show the general categorical relationships between the Functions. Protect, Detect, Respond, and
27 Recover from the Cybersecurity Framework are greyed out in this figure as they are not part of the
28 Privacy Framework, but organizations can find these Functions in the Cybersecurity Framework, and use
29 them to support the management of the data security aspect of privacy risk. Throughout the Core's
30 Categories and Subcategories, NIST added several examples in the form of parentheticals to make the
31 outcome statements more readily understood by organizations. The table below provides a summary of
32 material changes only. Clarifying or editorial edits to the text are not included.
33

| Function | Material Changes |
|--------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Identify (ID-P) | <i>Inventory and Mapping</i> (ID.IM-P) <ul style="list-style-type: none"> Added two Subcategories: ID.IM-P3 and ID.IM-P5 (previously ID.RA-P1) |
| | <i>Business Environment</i> (ID.BE-P) <ul style="list-style-type: none"> Changed use of the term "supply chain risk management" to "data processing ecosystem" in ID.BE-P1; "data processing ecosystem" is now a defined term in the updated Glossary |

| Function | Material Changes |
|------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| | <p><i>Risk Assessment</i> (ID.RA-P)</p> <ul style="list-style-type: none"> Relocated and modified ID.RA-P2 (previously IN.AW-P7) from Inform Relocated ID.RA-P1 to Inventory and Mapping (see above) <p><i>Data Processing Ecosystem Risk Management</i> (ID.DE-P)</p> <ul style="list-style-type: none"> Changed use of the term “supply chain” terminology to “data processing ecosystem” terminology throughout the Core and changed identifiers from SC to DE; “data processing ecosystem” is now a defined term in the updated Glossary Added a new Subcategory ID.DE-P4 Removed previous ID.SC-P5 because it is sufficiently addressed by ID.DE-P5 |
| <p>Govern (GV-P) [New Function]</p> | <p><i>Governance Policies, Processes, and Procedures</i> (GV.PP-P)</p> <ul style="list-style-type: none"> Relocated this Category from Identify (previously Governance [ID.GV-P]) <p><i>Risk Management Strategy</i> (GV.RM-P)</p> <ul style="list-style-type: none"> Relocated this Category from Identify (previously ID.RM-P) <p><i>Awareness and Training</i> (GV.AT-P)</p> <ul style="list-style-type: none"> Relocated this Category from Protect (previously PR.AT-P) <p><i>Monitoring</i> (GV.MT-P) [New Category]</p> <ul style="list-style-type: none"> Created new Category statement Created seven Subcategories: GV.MT-P1 (previously ID.RA-P6) was relocated from Identify; three new Subcategories (GV.MT-P2 through P4); and GV.MT-P5, GV.MT-P6, and GV.MT-P7 (previously RS.AN-P5, RS.IM-P1, and RS.RE-P1, respectively) were relocated from Respond |
| <p>Protect (PR-P) [Removed]</p> | <ul style="list-style-type: none"> Removed Protect Function, but relocated Awareness and Training (previously PR.AT-P) and Protected Processing (previously PR.PP-P) to Govern and Control, respectively |
| <p>Control (CT-P)</p> | <p><i>Data Management Policies, Processes, and Procedures</i> (CT.PO-P)</p> <ul style="list-style-type: none"> Modified CT.PO-P1 to address individual consent and revocation and incorporate the previous CT.DM-P2 Relocated and modified CT.PO-P4 (previously PR.DP-P2) from Protect <p><i>Data Management</i> (CT.DM-P)</p> <ul style="list-style-type: none"> Relocated CT.DM-P5 and P8 (previously PR.DP-P6 and PR.PT-P1, respectively) from Protect <p><i>Data Minimization</i> (CT.MN-P) [New Category]</p> <ul style="list-style-type: none"> Renamed Category (previously Protected Processing [PR.PP-P]) Created seven Subcategories: CT.MN-P1 through P5 (previously PR.PP-P1 through P5) were relocated from Protected Processing in Protect; CT.MN-P6 (previously CT.DM-P1) was relocated from Data Management in Control; and CT.MN-P7 (previously PR.AC-P7) was relocated from Identity Management, Authentication, and Access Control in Protect |

| Function | Material Changes |
|------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Communicate (CM-P) [Previously Inform (IN-P)] | <p><i>Communication Policies, Processes, and Procedures (CM.PP-P)</i></p> <ul style="list-style-type: none"> Renamed Category (previously Transparency Processes and Procedures [IN.TP-P]) Modified CM.PP-P1 to incorporate policies, processes and procedures for communicating (previously addressed by two Subcategories, IN.TP-P1 and P2) Added new Subcategory CM.PP-P2 to address communication roles and responsibilities |
| | <p><i>Data Processing Awareness (CM.AW-P)</i></p> <ul style="list-style-type: none"> Modified CM.AW-P1 (previously IN.AW-P2) to focus on mechanisms for communicating and included examples of such mechanisms Modified CM.AW-P4 (previously IN.AW-P1) to include records of data disclosures can be accessed for review or transmission/disclosure Modified CM.AW-P5 and combined two Subcategories (previous IN.AW-P4 and P5) to include communication of data corrections or deletions to both individuals and organizations (e.g., data sources) Modified CM.AW-P6 to add data lineage and capability for access for review or transmission/disclosure Relocated CM.AW-P7 and P8 (previously RS.CO-P6 and RS.RE-P2, respectively) from Respond |
| Respond (RS-P) [Removed] | <ul style="list-style-type: none"> Removed Respond Function, but relocated some Subcategories to Govern and Communicate (see above) |

34 Appendix A: Privacy Framework Core

35 This appendix presents the Core: a table of Functions, Categories, and Subcategories that describe
36 specific privacy activities that can support managing privacy risks when systems, products, and services
37 are processing data.

38 Notes to Users

39 Under the Privacy Framework's risk-based approach:

- 40 1. An organization may not need to achieve every outcome or activity reflected in the Core. It is
41 expected that an organization will use Profiles to select and prioritize the Functions, Categories,
42 and Subcategories that best meet its specific needs by considering its organizational or industry
43 sector goals, legal/regulatory requirements and industry best practices, the organization's risk
44 management priorities, and the privacy needs of individuals who are directly or indirectly served
45 or affected by the organization's systems, products, or services. **Thus, the Subcategories should**
46 **not be read as a checklist in isolation from their Categories, which often provide a risk-based**
47 **modifier on Subcategory selection.**
- 48 2. It is not obligatory to achieve an outcome in its entirety. An organization may use its Profiles to
49 express partial achievement of an outcome, as not all aspects of an outcome may be relevant
50 for the organization to manage privacy risk, or the organization may use a Target Profile to
51 express an aspect of an outcome that it doesn't currently have the capability to achieve.
- 52 1) It may be necessary to consider multiple outcomes in combination in order to appropriately
53 manage privacy risk. For example, an organization that responds to individuals' requests for data
54 access may select for its Profile both the Subcategory: *CT.DM-P1: Data elements can be*

55 *accessed for review and the Category: Identity Management, Authentication, and Access Control*
 56 *(PR.AC-P)* to ensure that only the individual to whom the data pertain gets access.

57 **Implementation:** The table format of the Core is not intended to suggest a specific implementation
 58 order or imply a degree of importance between the Functions, Categories and Subcategories.
 59 Implementation may be non-sequential, simultaneous, or iterative, depending on the SDLC stage, status
 60 of the privacy program, or scale of the workforce. In addition, the Core is not exhaustive; it is extensible,
 61 allowing organizations, sectors, and other entities to adapt or add additional Functions, Categories and
 62 Subcategories to their Profiles.

63 **Roles:**

- 64 • **Workforce:** Different parts of an organization’s workforce may take responsibility for different
 65 Categories or Subcategories. For example, the legal department may be responsible for carrying
 66 out activities under Governance Processes and Procedures while the IT department is working
 67 on Inventory and Mapping. Ideally, the Core encourages cross-organization collaboration to
 68 develop Profiles and achieve outcomes.
- 69 • **Ecosystem:** The Core is intended to be usable by any organization or entity regardless of its role
 70 in the data processing ecosystem. Although the Privacy Framework does not classify ecosystem
 71 roles, an organization should review the Core from its standpoint in the ecosystem. An
 72 organization’s role(s) may be legally codified – for example, some laws classify organizations as
 73 data controllers or data processors – or classifications may be derived from industry
 74 designations. Since Core elements are not assigned by ecosystem role, an organization can use
 75 its Profiles to select Functions, Categories, and Subcategories that are relevant to its role(s).

76 **Scalability:** Certain aspects of outcomes may be ambiguously worded. For example, outcomes may
 77 include terms like “communicated” or “disclosed” without stating to whom the communications or
 78 disclosures are being made. The ambiguity is intentional to allow for a wide range of organizations with
 79 different use cases to determine what is appropriate or required in a given context.

80 **Resource Repository:** Additional supporting resources, including informative references that can
 81 provide more guidance on how to achieve an outcome can be found on the NIST website at
 82 <https://www.nist.gov/privacy-framework>.

83 **Cybersecurity Framework Alignment:**

- 84 • **Figure 1** shows the general categorical relationships between the Functions: Identify and Govern
 85 are primarily organizational-level or contain foundational outcomes and activities. Control,
 86 Communicate, and Protect are primarily system/product/service-level and contain outcomes
 87 and activities that may not be applicable for all systems, products, and services or to the same
 88 degree, and Detect, Respond, and Recover are primarily incident-related. The Functions Protect,
 89 Detect, Respond, and Recover are greyed out in **Figure 1** and **Table 1** as they are not part of the
 90 Privacy Framework, but organizations can find these Functions in the Cybersecurity Framework,
 91 and use them to support the management of the data security aspect of privacy risk.
- 92 • Certain Functions, Categories, or Subcategories are identical to or have been adapted from the
 93 Cybersecurity Framework. The following legend can be used to identify this relationship in **Table**
 94 **2**.

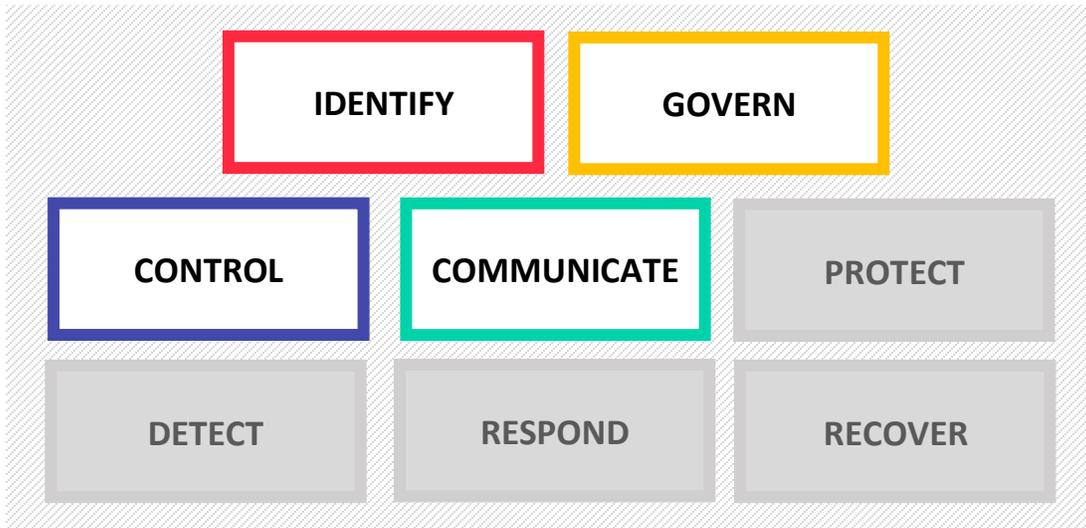
95  The Function, Category, or Subcategory aligns with the Cybersecurity
 Framework, but the text has been adapted for the Privacy Framework.

96  The Category or Subcategory is identical to the Cybersecurity
 Framework.

97 **Core Identifiers:** For ease of use, each component of the Core is given a unique identifier. Functions and
 98 Categories each have a unique alphabetic identifier, as shown in **Table 1**. Subcategories within each
 99 Category have a number added to the alphabetic identifier; the unique identifier for each Subcategory is
 100 included in **Table 2**.

101

Figure 1: Privacy and Cybersecurity Framework Functions



102

103

Table 1: Privacy and Cybersecurity Framework Function and Category Unique Identifiers

| Function Unique Identifier | Function | Category Unique Identifier | Category |
|----------------------------|---------------|----------------------------|-----------------------------------------------------|
| ID-P | Identify-P | ID.IM-P | Inventory and Mapping |
| | | ID.BE-P | Business Environment |
| | | ID.RA-P | Risk Assessment |
| | | ID.DE-P | Data Processing Ecosystem Risk Management |
| GV-PP | Govern-P | GV.PP-P | Governance Policies, Processes, and Procedures |
| | | GV.RM-P | Risk Management Strategy |
| | | GV.AT-P | Awareness and Training |
| | | GV.MT-P | Monitoring |
| CT-P | Control-P | CT.PO-P | Data Management Policies, Processes, and Procedures |
| | | CT.DM-P | Data Management |
| | | CT.MN-P | Data Minimization |
| CM-P | Communicate-P | CM.PP-P | Communication Policies, Processes, and Procedures |

| | | | | |
|-----------|---------|--|---------|-------------------------------------------------|
| | | | CM.AW-P | Data Processing Awareness |
| PR | Protect | | PR.AC | Identity Management and Access Control |
| | | | PR.AT | Awareness and Training |
| | | | PR.DS | Data Security |
| | | | PR.IP | Information Protection Processes and Procedures |
| | | | PR.MA | Maintenance |
| | | | PR.PT | Protective Technology |
| DE | Detect | | DE.AE | Anomalies and Events |
| | | | DE.CM | Security Continuous Monitoring |
| | | | DE.DP | Detection Processes |
| RS | Respond | | RS.RP | Response Planning |
| | | | RS.CO | Communications |
| | | | RS.AN | Analysis |
| | | | RS.MI | Mitigation |
| | | | RS.IM | Improvements |
| RC | Recover | | RC.RP | Recovery Planning |
| | | | RC.IM | Improvements |
| | | | RC.CO | Communications |

Table 2: Privacy Framework Core

| Function | Category | Subcategory |
|------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| IDENTIFY-P (ID-P): Develop the organizational understanding to manage privacy risk for individuals arising from system, product, or service data processing. | Inventory and Mapping (ID.IM-P): Data processing by systems, products, or services are understood and inform the management of privacy risk. | ID.IM-P1: Systems/products/services that process data are inventoried. |
| | | ID.IM-P2: Owners or operators (e.g., the organization or third parties such as service providers, partners, customers, developers, etc.) and their roles with respect to the systems/products/services and components (e.g., internal or external) that process data are inventoried. |
| | | ID.IM-P3: Categories of individuals (e.g., customers, employees or prospective employees, consumers, second tier customers) whose data are being processed are inventoried. |
| | | ID.IM-P4: Data actions of the systems/products/services are inventoried. |
| | | ID.IM-P5: The purposes for the data actions are inventoried. |
| | | ID.IM-P6: Data elements within the data actions are inventoried. |
| | | ID.IM-P7: The data processing environment is understood (e.g., geographic location, internal, cloud, third parties). |
| | | ID.IM-P8: Data processing is mapped, illustrating the data actions and associated data elements by systems/products/services, including components (e.g., internal or external); roles of the component owners/operators; and interactions of individuals or third parties with the systems/products/services. |
| | Business Environment (ID.BE-P): The organization’s mission, objectives, stakeholders, and activities are understood and prioritized; this information is used to inform privacy roles, responsibilities, and risk management decisions. | ID.BE-P1: The organization’s role in the data processing ecosystem is identified and communicated. |
| | | ID.BE-P2: Priorities for organizational mission, objectives, and activities are established and communicated. |
| | | ID.BE-P3: Systems/products/services that support organizational priorities are identified and key functional requirements communicated. |
| | Risk Assessment (ID.RA-P): The organization understands the privacy risks to individuals and how such privacy risks may create secondary impacts on | ID.RA-P1: Contextual factors related to the systems/products/services and the data actions are identified (e.g., individuals’ demographics and privacy interests or perceptions, data sensitivity, visibility of data processing to individuals and third parties). |

| Function | Category | Subcategory |
|------------------------------------------------------------------------------------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| | organizational operations, including mission, functions, other risk management priorities (e.g. compliance, financial), reputation, workforce, and culture. | ID.RA-P2: Data analytic inputs and outputs are identified and evaluated for bias. |
| | | ID.RA-P3: Potential problematic data actions and associated problems are identified. |
| | | ID.RA-P4: Problematic data actions, likelihoods, and impacts are used to determine and prioritize risk. |
| | | ID.RA-P5: Risk responses are identified, prioritized, and implemented. |
| | Data Processing Ecosystem Risk Management (ID.DE-P): The organization’s priorities, constraints, risk tolerances, and assumptions are established and used to support risk decisions associated with managing privacy risk and third parties within the data processing ecosystem. The organization has established and implemented the processes to identify, assess, and manage privacy risks within the data processing ecosystem. | ID.DE-P1: Data processing ecosystem risk management processes are identified, established, assessed, managed, and agreed to by organizational stakeholders. |
| | | ID.DE-P2: Data processing ecosystem parties (e.g., service providers, customers, partners, product manufacturers, application developers) are identified, prioritized, and assessed using a privacy risk assessment process. |
| | | ID.DE-P3: Contracts with data processing ecosystem parties are used to implement appropriate measures designed to meet the objectives of an organization’s privacy program. |
| | | ID.DE-P4: Interoperability frameworks or similar multi-party approaches are used to manage data processing ecosystem privacy risks. |
| | | ID.DE-P5: Data processing ecosystem parties are routinely assessed using audits, test results, or other forms of evaluations to confirm they are meeting their contractual or framework obligations. |
| | | GOVERN-P (GV-P): Develop and implement the organizational governance structure to enable an |
| GV.PP-P2: Processes to instill organizational privacy values within system/product/service development and operations are established and in place. | | |
| GV.PP-P3: Roles and responsibilities for the workforce are established with respect to privacy. | | |

| Function | Category | Subcategory |
|-----------------------------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| ongoing understanding of the organization’s risk management priorities that are informed by privacy risk. | | GV.PP-P4: Privacy roles and responsibilities are coordinated and aligned with third-party stakeholders (e.g., service providers, customers, partners). |
| | | GV.PP-P5: Legal, regulatory, and contractual requirements regarding privacy are understood and managed. |
| | | GV.PP-P6: Governance and risk management policies, processes and procedures address privacy risks. |
| | Risk Management Strategy (GV.RM-P): The organization’s priorities, constraints, risk tolerances, and assumptions are established and used to support operational risk decisions. | GV.RM-P1: Risk management processes are established, managed, and agreed to by organizational stakeholders. |
| | | GV.RM-P2: Organizational risk tolerance is determined and clearly expressed. |
| | | GV.RM-P3: The organization’s determination of risk tolerance is informed by its role in the data processing ecosystem. |
| | Awareness and Training (GV.AT-P): The organization’s workforce and third parties engaged in data processing are provided privacy awareness education and are trained to perform their privacy-related duties and responsibilities consistent with related policies, processes, procedures, and agreements and organizational privacy values. | GV.AT-P1: The workforce is informed and trained on its roles and responsibilities. |
| | | GV.AT-P2: Senior executives understand their roles and responsibilities. |
| | | GV.AT-P3: Privacy personnel understand their roles and responsibilities. |
| | | GV.AT-P4: Third parties (e.g., service providers, customers, partners) understand their roles and responsibilities. |
| | Monitoring (GV.MT-P): The policies, processes, and procedures for ongoing review of the organization’s privacy posture are understood and inform the management of privacy risk. | GV.MT-P1: Privacy risk is re-evaluated on an ongoing basis and as key factors, including the organization’s business environment, governance (e.g., legal obligations, risk tolerance), data processing, and systems/products/services change. |
| | | GV.MT-P2: Privacy values and policies are reviewed and any updates are communicated. |
| | | GV.MT-P3: Policies, processes, and procedures for auditing compliance with legal requirements and privacy policies are established and in place. |

| Function | Category | Subcategory |
|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| | | GV.MT-P4: Policies, processes, and procedures for communicating progress on managing privacy risks are established and in place. |
| | | GV.MT-P5: Policies, processes, and procedures are established and in place to receive, analyze, and respond to problematic data actions disclosed to the organization from internal and external sources (e.g., internal discovery, privacy researchers). |
| | | GV.MT-P6: Policies, processes, and procedures incorporate lessons learned from problematic data actions. |
| | | GV.MT-P7: Policies, processes, and procedures for receiving, tracking, and responding to complaints, concerns, and questions from individuals about organizational privacy practices are established and in place. |
| CONTROL-P (CT-P): Develop and implement appropriate activities to enable organizations or individuals to manage data with sufficient granularity to manage privacy risks. | Data Management Policies, Processes, and Procedures (CT.PO-P): Policies, processes, and procedures are maintained and used to manage data processing (e.g., purpose, scope, roles, responsibilities, management commitment, and coordination among organizational entities) consistent with the organization’s risk strategy to protect individuals’ privacy. | CT.PO-P1: Policies, processes, and procedures for authorizing data processing (e.g., organizational decisions, individual consent), revoking authorizations, and maintaining authorizations are established and in place. |
| | | CT.PO-P2: Policies, processes, and procedures for enabling data review, transmission or disclosure, alteration, and deletion are established and in place. |
| | | CT.PO-P3: Policies, processes, and procedures for enabling individuals’ data processing preferences and requests are established and in place. |
| | | CT.PO-P4: An information life cycle to manage data is aligned and implemented with the system development life cycle to manage systems. |
| | Data Management (CT.DM-P): Data are managed consistent with the organization's risk strategy to protect individuals’ privacy, increase manageability, and enable the implementation of privacy principles (e.g., individual participation, data quality, data minimization). | CT.DM-P1: Data elements can be accessed for review. |
| | | CT.DM-P2: Data elements can be accessed for transmission or disclosure. |
| | | CT.DM-P3: Data elements can be accessed for alteration. |
| | | CT.DM-P4: Data elements can be accessed for deletion. |
| | | CT.DM-P5: Data are destroyed according to policy. |
| | | CT.DM-P6: Data are transmitted using standardized formats. CT.DM-P7: Metadata containing processing permissions and related data values are transmitted with data elements. |

| Function | Category | Subcategory |
|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| | <p>Data Minimization (CT.MN-P): Technical data processing solutions increase disassociability consistent with related policies, processes, procedures, and agreements and the organization’s risk strategy to protect individuals’ privacy.</p> | <p>CT.DM-P8: Audit/log records are determined, documented, implemented, and reviewed in accordance with policy and incorporating the principle of data minimization.</p> |
| | | <p>CT.MN-P1: Data are processed in an unobservable or unlinkable manner.</p> |
| | | <p>CT.MN-P2: Data are processed to limit the identification of individuals.</p> |
| | | <p>CT.MN-P3: Data are processed to restrict the formulation of inferences about individuals’ behavior or activities.</p> |
| | | <p>CT.MN-P4: Data processing is decentralized.</p> |
| | | <p>CT.MN-P5: Data actions take place on local devices.</p> |
| | | <p>CT.MN-P6: System or device configurations permit selective collection or disclosure of data elements.</p> |
| <p>COMMUNICATE -P (CM-P): Develop and implement appropriate activities to enable organizations and individuals to have a reliable understanding about how data are processed and associated privacy risks.</p> | <p>Communication Policies, Processes, and Procedures (CM.PP-P): Policies, processes, and procedures are maintained and used to increase transparency of the organization’s data processing practices (e.g., purpose, scope, roles, responsibilities, management commitment, and coordination among organizational entities) and associated privacy risks.</p> | <p>CM.PP-P1: Transparency policies, processes, and procedures for communicating data processing purposes, practices, and associated privacy risks are established and in place.</p> |
| | | <p>CM.PP-P2: Roles and responsibilities (e.g., public relations) for communicating data processing purposes, practices, and associated privacy risks are established.</p> |
| | <p>Data Processing Awareness (CM.AW-P): Individuals and organizations have reliable knowledge about data processing practices and associated privacy risks, and mechanisms are used and maintained to increase predictability consistent with the organization’s risk strategy to protect individuals’ privacy.</p> | <p>CM.AW-P1: Mechanisms (e.g., notices, internal or public reports) for communicating data processing purposes, practices, associated privacy risks, and options for enabling individuals’ data processing preferences and requests are established and in place.</p> |
| | | <p>CM.AW-P2: Mechanisms for obtaining feedback from individuals (e.g., surveys or focus groups) about data processing and associated privacy risks are established and in place.</p> |
| | | <p>CM.AW-P3: System/product/service design enables data processing visibility.</p> |

| | Function | Category | Subcategory |
|--|----------|----------|------------------------------------------------------------------------------------------------------------------------------------------------|
| | | | <p>CM.AW-P4: Records of data disclosures are maintained and can be accessed for review or transmission/disclosure.</p> |
| | | | <p>CM.AW-P5: Data corrections or deletions can be communicated to individuals or organizations (e.g., data sources).</p> |
| | | | <p>CM.AW-P6: Data lineage and provenance are maintained and can be accessed for review or transmission/disclosure.</p> |
| | | | <p>CM.AW-P7: Impacted individuals and organizations are notified about a privacy breach or event.</p> |
| | | | <p>CM.AW-P8: Individuals are provided with mitigation mechanisms to address impacts to individuals that arise from data processing.</p> |

106