NIST Informative References for the Privacy Framework: A Tool for Improving Privacy through Enterprise Risk Management
Preliminary Draft

Note to Reviewers
NIST welcomes feedback on the appropriateness of the listed guidance, as well as additional relevant NIST guidance.

The NIST Privacy Framework: A Tool for Improving Privacy through Enterprise Risk Management (Privacy Framework) permits any organization or industry sector to map the outcome-based Subcategories in the Core to standards, guidelines, and practices to support the achievement of the outcomes associated with each Subcategory. In Table 1, NIST provides a mapping of the Subcategories to key relevant NIST guidance. Appendix A provides citations for the NIST guidance used in this mapping. This mapping is not intended to be comprehensive.

Table 1: NIST Informative References

	Function	Category	Subcategory	NIST Informative References
	IDENTIFY-P (ID-P): Develop the organizational understanding to manage privacy risk for individuals arising from data processing.	**Inventory and Mapping (ID.IM-P):** Data processing by systems, products, or services is understood and informs the management of privacy risk.	**ID.IM-P1:** Systems/products/services that process data are inventoried.	**NIST SP 800-37 Rev. 2:** Task P-10 **NIST SP 800-53 Rev. 5 (draft):** CM-8 (10), CM-12 **NISTIR 8062** **NIST PRAM:** Worksheet 2
			ID.IM-P2: Owners or operators (e.g., the organization or third parties such as service providers, partners, customers, and developers) and their roles with respect to the systems/products/services and components (e.g., internal or external) that process data are inventoried.	**NIST SP 800-37 Rev. 2:** Task P-9, P-10 **NIST SP 800-53 Rev. 5 (draft):** CM-8 (10) **NISTIR 8062** **NIST PRAM:** Worksheet 2
			ID.IM-P3: Categories of individuals (e.g., customers, employees or	**NISTIR 8062** **NIST PRAM:** Worksheet 2

	Function	Category	Subcategory	NIST Informative References
			prospective employees, consumers) whose data are being processed are inventoried.	
			ID.IM-P4: Data actions of the systems/products/services are inventoried.	**NIST SP 800-37 Rev. 2:** Task P-13 **NIST SP 800-53 Rev. 5 (draft):** CM-8(10) **NISTIR 8062** **NIST PRAM:** Worksheet 2
			ID.IM-P5: The purposes for the data actions are inventoried.	**NIST SP 800-37 Rev. 2:** Task P-13 **NIST SP 800-53 Rev. 5 (draft):** CM-8(10), PA-1, PA-2, PA-3
			ID.IM-P6: Data elements within the data actions are inventoried.	**NIST SP 800-37 Rev. 2:** Task P-12 **NIST SP 800-53 Rev. 5 (draft):** CM-8(10), CM-12, PM-29 **NISTIR 8062** **NIST PRAM:** Worksheet 2
			ID.IM-P7: The data processing environment is identified (e.g., geographic location, internal, cloud, third parties).	**NIST SP 800-37 Rev. 2:** Task P-16 **NIST SP 800-53 Rev. 5 (draft):** CM-8(10), RA-2 **NISTIR 8062** **NIST PRAM:** Worksheet 2
			ID.IM-P8: Data processing is mapped, illustrating the data actions and associated data elements for systems/products/services, including components; roles of the component owners/operators; and interactions of individuals or third parties with the systems/products/services.	**NIST SP 800-37 Rev. 2:** Task P-13 **NIST SP 800-53 Rev. 5 (draft):** CM-8(10) **NISTIR 8062** **NIST PRAM:** Worksheet 2
		Business Environment (ID.BE-P): The organization's mission, objectives, stakeholders,	**ID.BE-P1:** The organization's role in the data processing ecosystem is identified and communicated.	**NIST SP 800-37 Rev. 2:** Section 2.8 Supply Chain Risk Management, Task P-9 **NIST SP 800-53 Rev. 5 (draft):** CP-2, SA-12 **NIST SP 800-161**

	Function	Category	Subcategory	NIST Informative References
		and activities are understood and prioritized; this information is used to inform privacy roles, responsibilities, and risk management decisions.		**NISTIR 7622**
			ID.BE-P2: Priorities for organizational mission, objectives, and activities are established and communicated.	**NIST SP 800-37 Rev. 2:** Task P-8 **NIST SP 800-53 Rev. 5 (draft):** PM-11 **NIST PRAM:** Worksheet 1
			ID.BE-P3: Systems/products/services that support organizational priorities are identified and key requirements communicated.	**NIST SP 800-37 Rev. 2:** Task P-8 **NIST SP 800-53 Rev. 5 (draft):** RA-9 **NIST PRAM:** Worksheet 1
		Risk Assessment (ID.RA-P): The organization understands the privacy risks to individuals and how such privacy risks may create follow-on impacts on organizational operations, including mission, functions, other risk management priorities (e.g., compliance, financial), reputation, workforce, and culture.	**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).	**NIST SP 800-37 Rev. 2:** Task P-9 **NISTIR 8062** **NIST PRAM:** Worksheet 2
			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.	**NIST SP 800-30 Rev. 1** **NIST SP 800-37 Rev. 2:** Task P-9 **NIST SP 800-53 Rev. 5 (draft):** CM-4, RA-3 **NISTIR 8062** **NIST PRAM:** Worksheet 3, Catalog of Problematic Data Actions and Problems
			ID.RA-P4: Problematic data actions, likelihoods, and impacts are used to determine and prioritize risk.	**NIST SP 800-30 Rev. 1** **NIST SP 800-37 Rev. 2:** Task P-14 **NIST SP 800-39** **NIST SP 800-53 Rev. 5 (draft):** RA-3 **NISTIR 8062**

	Function	Category	Subcategory	NIST Informative References
				NIST PRAM: Worksheet 3, Catalog of Problematic Data Actions and Problems
			ID.RA-P5: Risk responses are identified, prioritized, and implemented.	**NIST SP 800-30 Rev. 1** **NIST SP 800-37 Rev. 2:** Task P-14, R-3 **NIST SP 800-39** **NIST SP 800-53 Rev. 5 (draft):** RA-7 **NISTIR 8062** **NIST PRAM:** Worksheet 4
		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.	**NIST SP 800-37 Rev. 2:** Section 2.8, Task P-2 **NIST SP 800-53 Rev. 5 (draft):** SA-12, PM-31 **NIST SP 800-161** **NISTIR 7622**
			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.	**NIST SP 800-30 Rev. 1** **NIST SP 800-53 Rev. 5 (draft):** RA-3(1), SA-12 **NIST SP 800-161** **NISTIR 7622**
			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.	**NIST SP 800-53 Rev. 5 (draft):** PM-31, SA-12(1) **NIST SP 800-161** **NISTIR 7622**
			ID.DE-P4: Interoperability frameworks or similar multi-party approaches are used to manage data processing ecosystem privacy risks.	**NISTIR 8149**

	Function	Category	Subcategory	NIST Informative References
			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.	**NIST SP 800-53 Rev. 5 (draft):** SA-12(2) **NIST SP 800-161** **NISTIR 7622**
	GOVERN-P (GV-P): 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.	**Governance Policies, Processes, and Procedures (GV.PP-P):** The policies, processes, and procedures to manage and monitor the organization's regulatory, legal, risk, environmental, and operational requirements are understood and inform the management of privacy risk.	**GV.PP-P1:** Organizational privacy values and policies (e.g., conditions on data processing, individuals' prerogatives with respect to data processing) are established and communicated.	**NIST SP 800-39** **NIST SP 800-53 Rev. 5 (draft):** all -1 controls, PM-23 **NIST PRAM:** Worksheet 1
			GV.PP-P2: Processes to instill organizational privacy values within system/product/service development and operations are established and in place.	**NIST SP 800-53 Rev. 5 (draft):** PM-6 **NIST PRAM:** Worksheet 1
			GV.PP-P3: Roles and responsibilities for the workforce are established with respect to privacy.	**NIST SP 800-37 Rev. 2:** Task P-1, Appendix D **NIST SP 800-53 Rev. 5 (draft):** PM-3
			GV.PP-P4: Privacy roles and responsibilities are coordinated and aligned with third-party stakeholders (e.g., service providers, customers, partners).	**NIST SP 800-37 Rev. 2:** Task P-1, Appendix D **NIST SP 800-53 Rev. 5 (draft):** IR-4, PM-3, PM-18 , PM-19
			GV.PP-P5: Legal, regulatory, and contractual requirements regarding privacy are understood and managed.	**NIST SP 800-37 Rev. 2:** Task P-4, P-15 **NIST SP 800-53 Rev. 5 (draft):** PM-30 **NIST PRAM:** Worksheet 1
			GV.PP-P6: Governance and risk management policies, processes,	**NIST SP 800-37 Rev. 2:** Task P-15, P-16 **NIST SP 800-39**

	Function	Category	Subcategory	NIST Informative References
			and procedures address privacy risks.	**NIST SP 800-53 Rev. 5 (draft):** PM-3, PM-7, PM-9, PM-10, PM-11, PM-18, PM-19, PM-21, PM-22, PM-23, PM-24, PM-25, PM-26, PM-28, PM-29, PM-30 **NIST PRAM:** Worksheet 1
		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.	**NIST SP 800-37 Rev. 2:** Task P-2 **NIST SP 800-39** **NIST SP 800-53 Rev. 5 (draft):** PM-9
			GV.RM-P2: Organizational risk tolerance is determined and clearly expressed.	**NIST SP 800-37 Rev. 2:** Task P-2 **NIST SP 800-39** **NIST SP 800-53 Rev. 5 (draft):** PM-9, PM-32
			GV.RM-P3: The organization's determination of risk tolerance is informed by its role in the data processing ecosystem.	**NIST SP 800-37 Rev. 2:** Task P-2 **NIST SP 800-39** **NIST SP 800-53 Rev. 5 (draft):** PM-32
		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.	**NIST SP 800-53 Rev. 5 (draft)**: AT-2, AT-3, PM-13
			GV.AT-P2: Senior executives understand their roles and responsibilities.	**NIST SP 800-37 Rev. 2:** Task P-1 **NIST SP 800-53 Rev. 5 (draft):** AT-3, PM-13
			GV.AT-P3: Privacy personnel understand their roles and responsibilities.	**NIST SP 800-37 Rev. 2:** Task P-1 **NIST SP 800-53 Rev. 5 (draft):** AT-3, PM-13
			GV.AT-P4: Third parties (e.g., service providers, customers, partners) understand their roles and responsibilities.	**NIST SP 800-53 Rev. 5 (draft):** PS-7, SA-9, SA-12 (1) **NIST SP 800-161** **NISTIR 7622**
		Monitoring and Review (GV.MT-P): The policies,	**GV.MT-P1:** Privacy risk is re-evaluated on an ongoing basis and	**NIST SP 800-37 Rev. 2:** Task P-14, S-5, M-1, M-2 **NIST SP 800-53 Rev. 5 (draft):** CA-7, PM-29

	Function	Category	Subcategory	NIST Informative References
		processes, and procedures for ongoing review of the organization's privacy posture are understood and inform the management of privacy risk.	as key factors, including the organization's business environment, governance (e.g., legal obligations, risk tolerance), data processing, and systems/products/services change.	**NISTIR 8062**
			GV.MT-P2: Privacy values, policies, and training are reviewed and any updates are communicated.	**NIST SP 800-53 Rev. 5 (draft):** AT-1(8), AT-2
			GV.MT-P3: Policies, processes, and procedures for assessing compliance with legal requirements and privacy policies are established and in place.	**NIST SP 800-37 Rev. 2:** Task M-2 **NIST SP 800-53 Rev. 5 (draft):** PM-18 **NIST SP 800-53A Rev. 4:** all -1 controls
			GV.MT-P4: Policies, processes, and procedures for communicating progress on managing privacy risks are established and in place.	**NIST SP 800-37 Rev. 2:** Task M-5 **NIST SP 800-53 Rev. 5 (draft):** PM-18, PM-28, PM-29
			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).	**NIST SP 800-37 Rev. 2:** Task A-6, M-3 **NIST SP 800-53 Rev. 5 (draft):** CA-5, PM-15, SI-20(8)
			GV.MT-P6: Policies, processes, and procedures incorporate lessons learned from problematic data actions.	**NIST SP 800-53 Rev. 5 (draft):** all -1 controls, CP-2, IR-4, IR-8
			GV.MT-P7: Policies, processes, and procedures for receiving, tracking, and responding to complaints,	**NIST SP 800-53 Rev. 5 (draft):** IP-3, PM-28

	Function	Category	Subcategory	NIST Informative References
			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.	**NIST SP 800-53 Rev. 5 (draft):** AC-21, IP-2, PA-1, PA-2, PA-3, PA-4 **NIST SP 800-63-3**
			CT.PO-P2: Policies, processes, and procedures for enabling data review, transfer, sharing or disclosure, alteration, and deletion are established and in place.	**NIST SP 800-53 Rev. 5 (draft):** MP-6, MP-6(9), PM-23, PM-24, PM-26, PM-28, SI-12, SI-18, SI-19 **NIST SP 800-88 Rev. 1**
			CT.PO-P3: Policies, processes, and procedures for enabling individuals' data processing preferences and requests are established and in place.	**NIST SP 800-53 Rev. 5 (draft):** AC-1, IP-1, IP-2, IP-3, IP-4, IP-6, PM-27 **NIST SP 800-63-3**
			CT.PO-P4: An information life cycle to manage data is aligned and implemented with the system development life cycle to manage systems.	**NIST SP 800-37 Rev. 2:** Task P-13 **NIST SP 800-53 Rev. 5 (draft):** PL-8 SA-3, PM-23, PM-24, PM-25, SA-8, SA-12, SA-15, SA-17 SI-12 **NIST SP 800-160 Vol. 1**
		Data Management (CT.DM-P): Data are managed consistent with the organization's risk strategy to protect individuals' privacy, increase manageability,	**CT.DM-P1:** Data elements can be accessed for review.	**NIST SP 800-53 Rev. 5 (draft):** IP-6, PM-23, SI-12, SI-19
			CT.DM-P2: Data elements can be accessed for transmission or disclosure.	**NIST SP 800-53 Rev. 5 (draft):** IP-6, PM-23, SI-12, SI-19
			CT.DM-P3: Data elements can be accessed for alteration.	**NIST SP 800-53 Rev. 5 (draft):** PM-23, SI-12, SI-19

Function	Category	Subcategory	NIST Informative References
	and enable the implementation of privacy principles (e.g., individual participation, data quality, data minimization).	**CT.DM-P4:** Data elements can be accessed for deletion.	**NIST SP 800-53 Rev. 5 (draft):** MP-6, MP-6(9), PM-23, SI-12, SI-19 **NIST SP 800-88 Rev. 1**
		CT.DM-P5: Data are destroyed according to policy.	**NIST SP 800-53 Rev. 5 (draft):** MP-6 **NIST SP 800-88 Rev. 1**
		CT.DM-P6: Data are transmitted using standardized formats.	**NISTIR 8112**
		CT.DM-P7: Metadata containing processing permissions and related data values are transmitted with data elements.	**NIST SP 800-53 Rev. 5 (draft):** AC-16, IP-1, PA-1, PA-2, PA-3, PA-3(2), PM-23(1), PM-23(2), SC-16, SI-19(2) **NISTIR 8112**
		CT.DM-P8: Audit/log records are determined, documented, implemented, and reviewed in accordance with policy and incorporating the principle of data minimization.	**NIST SP 800-53 Rev. 5 (draft):** AU Control Family
	Disassociated Processing (CT.DP-P): Data processing solutions increase disassociability consistent with related policies, processes, procedures, and agreements and the organization's risk strategy to protect individuals' privacy.	**CT.DP-P1:** Data are processed in an unobservable or unlinkable manner (e.g., data actions take place on local devices, privacy-preserving cryptography).	**NIST SP 800-53 Rev. 5 (draft):** IA-8(6), MP-6 **NIST SP 800-63-3** **NIST SP 800-188 (draft)** **NISTIR 8053**
		CT.DP-P2: Data are processed to limit the identification of individuals (e.g., differential privacy techniques, tokenization).	**NIST SP 800-53 Rev. 5 (draft):** AC-23, IA-4(8), MP-6, SI-20 **NIST SP 800-63-3** **NIST SP 800-188 (draft)** **NISTIR 8053**
		CT.DP-P3: Data are processed to restrict the formulation of inferences about individuals' behavior or activities (e.g., data processing is decentralized, distributed architectures).	**NIST SP 800-53 Rev. 5 (draft):** AC-23, IA-8(6), MP-6, SI-20 **NIST SP 800-63-3** **NIST SP 800-188 (draft)** **NISTIR 8053**

	Function	Category	Subcategory	NIST Informative References
			CT.DP-P4: System or device configurations permit selective collection or disclosure of data elements.	**NIST SP 800-53 Rev. 5 (draft):** AC-21, SI-12, SI-12(1), SI-12(2), SC-42(5) **NIST SP 800-63-3** **NIST SP 800-188 (draft)** **NISTIR 8053**
			CT.DP-P5: Attribute references are substituted for attribute values.	**NIST SP 800-53 Rev. 5 (draft):** AC-16, IP-2(1) **NIST SP 800-63-3** **NISTIR 8062** **NISTIR 8112**
			CT.DP-P6: Data processing is limited to that which is relevant and necessary for a system/product/service to meet mission/business objectives.	**NIST SP 800-53 Rev. 5 (draft):** SC-42(5), SI-12(1), SI-12(2), SI-15(1), SI-20(1), PM-26, PM-29 **NIST SP 800-63-3**
	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.	**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.	**CM.PP-P1:** Transparency policies, processes, and procedures for communicating data processing purposes, practices, and associated privacy risks are established and in place.	**NIST SP 800-37 Rev. 2:** Task M-5 **NIST SP 800-53 Rev. 5 (draft):** CA-5 P, CM-4 S, IP-4, PA-3, PM-21, PM-30, RA-8
			CM.PP-P2: Roles and responsibilities (e.g., public relations) for communicating data processing purposes, practices, and associated privacy risks are established.	**NIST SP 800-37 Rev. 2:** Task P-1, Appendix D **NIST SP 800-53 Rev. 5:** PM-19, PM-30
		Data Processing Awareness (CM.AW-P):	**CM.AW-P1:** Mechanisms (e.g., notices, internal or public reports)	**NIST SP 800-53 Rev. 5 (draft):** AC-8, IP-4 , IP-5, PM-21, SC-42(4)

	Function	Category	Subcategory	NIST Informative References
		Individuals and organizations have reliable knowledge about data processing practices and associated privacy risks, and effective mechanisms are used and maintained to increase predictability consistent with the organization's risk strategy to protect individuals' privacy.	for communicating data processing purposes, practices, associated privacy risks, and options for enabling individuals' data processing preferences and requests are established and in place.	
			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.	**NIST SP 800-53 Rev. 5 (draft):** IP-3, PM-21 **NISTIR 8062**
			CM.AW-P3: System/product/service design enables data processing visibility.	**NIST SP 800-53 Rev. 5 (draft):** SC-42(4), IP-4
			CM.AW-P4: Records of data disclosures and sharing are maintained and can be accessed for review or transmission/disclosure.	**NIST SP 800-53 Rev. 5 (draft):** PM-22
			CM.AW-P5: Data corrections or deletions can be communicated to individuals or organizations (e.g., data sources) in the data processing ecosystem.	**NIST SP 800-53 Rev. 5 (draft):** PM-23, SI-19 **NISTIR 8112**
			CM.AW-P6: Data provenance and lineage are maintained and can be accessed for review or transmission/disclosure.	**NISTIR 8112**
			CM.AW-P7: Impacted individuals and organizations are notified about a privacy breach or event.	**NIST SP 800-53 Rev. 5 (draft):** IR-1, IR-7, IR-8

	Function	Category	Subcategory	NIST Informative References
			CM.AW-P8: Individuals are provided with mitigation mechanisms to address impacts to individuals that arise from data processing.	**NIST SP 800-53 Rev. 5 (draft):** IP-3
	PROTECT-P (PR-P): Develop and implement appropriate data processing safeguards.	**Identity Management, Authentication, and Access Control (PR.AC-P):** Access to data and devices is limited to authorized individuals, processes, and devices, and is managed consistent with the assessed risk of unauthorized access.	**PR.AC-P1:** Identities and credentials are issued, managed, verified, revoked, and audited for authorized individuals, processes, and devices.	**NIST SP 800-53 Rev. 5 (draft):** IA-4(4) **NIST SP 800-63-3**
			PR.AC-P2: Physical access to data and devices is managed.	**NIST SP 800-53 Rev. 5 (draft):** PE-2, PE-3, PE-4, PE-5, PE-6, PE-18, PE-20
			PR.AC-P3: Remote access is managed.	**FIPS Publication 199** **NIST SP 800-46 Rev. 2** **NIST SP 800-53 Rev. 5:** AC-17, AC-20 **NIST SP 800-77** **NIST SP 800-113** **NIST SP 800-114 Rev. 1** **NIST SP 800-121 Rev. 2**
			PR.AC-P4: Access permissions and authorizations are managed, incorporating the principles of least privilege and separation of duties.	**NIST SP 800-53 Rev. 5 (draft):** AC-1, AC-2, AC-3, AC-5 **NIST SP 800-162**
			PR.AC-P5: Network integrity is protected (e.g., network segregation, network segmentation).	**NIST SP 800-53 Rev. 5 (draft):** AC-4, SC-7
			PR.AC-P6: Individuals and devices are proofed and bound to credentials, and authenticated commensurate with the risk of the transaction (e.g., individuals'	**NIST SP 800-53 Rev. 5 (draft):** IA-12 **NIST SP 800-63-3**

	Function	Category	Subcategory	NIST Informative References
			security and privacy risks and other organizational risks).	
		Data Security (PR.DS-P): Data are managed consistent with the organization's risk strategy to protect individuals' privacy and maintain data confidentiality, integrity, and availability.	**PR.DS-P1:** Data-at-rest are protected.	**NIST SP 800-53 Rev. 5 (draft):** MP-8, SC-12, SC-28 **NIST SP 800-175B**
			PR.DS-P2: Data-in-transit are protected.	**NIST SP 800-53 Rev. 5 (draft):** SC-8, SC-11, SC-12 **NIST SP 800-175B**
			PR.DS-P3: Systems/products/services and associated data are formally managed throughout removal, transfers, and disposition.	**NIST SP 800-53 Rev. 5 (draft):** CM-8, MP-6, PE-16
			PR.DS-P4: Adequate capacity to ensure availability is maintained.	**NIST SP 800-53 Rev. 5 (draft):** AU-4, CP-2, SC-5
			PR.DS-P5: Protections against data leaks are implemented.	**NIST SP 800-53 Rev. 5 (draft):** AC-4, AC-5, AC-6, PE-19, PS-3, PS-6, SC-7, SC-8, SC-, SC-31, SI-4
			PR.DS-P6: Integrity checking mechanisms are used to verify software, firmware, and information integrity.	**NIST SP 800-53 Rev. 5 (draft):** SC-16, SI-7 **NIST SP 800-175B**
			PR.DS-P7: The development and testing environment(s) are separate from the production environment.	**NIST SP 800-53 Rev. 5 (draft):** CM-2(6)
			PR.DS-P8: Integrity checking mechanisms are used to verify hardware integrity.	**NIST SP 800-53 Rev. 5 (draft):** SA-10, SI-7
		Data Protection Policies, Processes, and Procedures (PR.DP-P): Security and privacy policies (which address purpose, scope, roles,	**PR.DP-P1:** A baseline configuration of information technology is created and maintained incorporating security principles (e.g., concept of least functionality).	**NIST SP 800-37 Rev. 2:** Task I-2 **NIST SP 800-53 Rev. 5 (draft):** CM-2, CM-3, CM-4, CM-5

	Function	Category	Subcategory	NIST Informative References
		responsibilities, management commitment, and coordination among organizational entities), processes, and procedures are maintained and used to manage the protection of data.	**PR.DP-P2:** Configuration change control processes are established and in place.	**NIST SP 800-53 Rev. 5 (draft):** CM-3, CM-4, SA-10
			PR.DP-P3: Backups of information are conducted, maintained, and tested.	**NIST SP 800-34 Rev. 1** **NIST SP 800-53 Rev. 5 (draft):** CP-4, CP-6, CP-9 **NIST SP 800-84**
			PR.DP-P4: Policy and regulations regarding the physical operating environment for organizational assets are met.	**NIST SP 800-53 Rev. 5 (draft):** PE-10, PE-12, PE-13, PE-15, PE-18
			PR.DP-P5: Protection processes are improved.	**NIST SP 800-37 Rev. 2:** all steps and tasks **NIST SP 800-39** **NIST SP 800-53 Rev. 5 (draft):** CA-2, CA-7, CP-2, IR-8, PL-2, PM-6
			PR.DP-P6: Effectiveness of protection technologies is shared.	**NIST SP 800-53 Rev. 5 (draft):** AC-21, CA-7, SI-4
			PR.DP-P7: Response plans (Incident Response and Business Continuity) and recovery plans (Incident Recovery and Disaster Recovery) are in place and managed.	**NIST SP 800-34 Rev. 1** **NIST SP 800-53 Rev. 5 (draft):** CP-2, CP-7, CP-12, CP-13, IR-7, IR-8, IR-9, PE-17 **NIST SP 800-61 Rev. 2**
			PR.DP-P8: Response and recovery plans are tested.	**NIST SP 800-34 Rev. 1** **NIST SP 800-53 Rev. 5 (draft):** CP-4, IR-3, PM-14 **NIST SP 800-84**
			PR.DP-P9: Privacy procedures are included in human resources practices (e.g., deprovisioning, personnel screening).	**NIST SP 800-53 Rev. 5 (draft):** PS-1, PS-2, PS-3, PS-4, PS-5, PS-6, PS-7, PS-8, SA-21
			PR.DP-P10: A vulnerability management plan is developed and implemented.	**NIST SP 800-30 Rev. 1** **NIST SP 800-53 Rev. 5 (draft):** RA-3, RA-5, SI-2
		Maintenance (PR.MA-P): System maintenance and	**PR.MA-P1:** Maintenance and repair of organizational assets are	**NIST SP 800-53 Rev. 5 (draft):** MA-2, MA-3, MA-5, MA-6

	Function	Category	Subcategory	NIST Informative References
		repairs are performed consistent with policies, processes, and procedures.	performed and logged, with approved and controlled tools.	
			PR.MA-P2: Remote maintenance of organizational assets is approved, logged, and performed in a manner that prevents unauthorized access.	**NIST SP 800-53 Rev. 5 (draft):** MA-4
		Protective Technology (PR.PT-P): Technical security solutions are managed to ensure the security and resilience of systems/products/services and associated data, consistent with related policies, processes, procedures, and agreements.	**PR.PT-P1:** Removable media is protected and its use restricted according to policy.	**NIST SP 800-53 Rev. 5 (draft):** MP-2, MP-3, MP-4, MP-5, MP-7, MP-8
			PR.PT-P2: The principle of least functionality is incorporated by configuring systems to provide only essential capabilities.	**NIST SP 800-53 Rev. 5 (draft):** AC-3, CM-7
			PR.PT-P3: Communications and control networks are protected.	**NIST SP 800-53 Rev. 5 (draft):** AC-4, AC-17, AC-18, CP-8, SC-7 SC-20, SC-21, SC-22, SC-23, SC-24, SC-25, SC-29, SC-32, SC-36, SC-37, SC-38, SC-39, SC-40, SC-41, SC-43
			PR.PT-P4: Mechanisms (e.g., failsafe, load balancing, hot swap) are implemented to achieve resilience requirements in normal and adverse situations.	**NIST SP 800-53 Rev. 5 (draft):** CP-7, CP-8, CP-11, CP-13, PL-8, RA-9

Appendix A: NIST Guidance References

1. Federal Information Processing Standards (FIPS) Publication 199, Standards for Security Categorization of Federal Information and Information Systems, https://doi.org/10.6028/NIST.FIPS.199

2. NIST Interagency Report (NISTIR) 7622, Notional Supply Chain Risk Management Practices for Federal Information Systems https://doi.org/10.6028/NIST.IR.7622

3. NIST Internal Report (NISTIR) 7966, Security of Interactive and Automated Access Management Using Secure Shell (SSH), https://doi.org/10.6028/NIST.IR.7966

4. NIST Internal Report (NISTIR) 8053, De-Identification of Personal Information, https://doi.org/10.6028/NIST.IR.8053

5. NIST Internal Report (NISTIR) 8062, An Introduction to Privacy Engineering and Risk Management in Federal Systems, https://doi.org/10.6028/NIST.IR.8062

6. NIST Internal Report (NISTIR) 8112, Attribute Metadata: A Proposed Schema for Evaluating Federated Attributes, https://doi.org/10.6028/NIST.IR.8112

7. NIST Interagency or Internal Report (NISTIR) 8149, Developing Trust Frameworks to Support Identity Federations, https://doi.org/10.6028/NIST.IR.8149

8. NIST Privacy Risk Assessment Methodology (PRAM), https://www.nist.gov/itl/applied-cybersecurity/privacy-engineering/resources

9. NIST Special Publication (SP) 800-30, Revision 1, Guide for Conducting Risk Assessments, https://doi.org/10.6028/NIST.SP.800-30r1

10. NIST SP 800-34, Revision 1, Contingency Planning Guide for Federal Information Systems, https://doi.org/10.6028/NIST.SP.800-34r1

11. NIST SP 800-37, Revision 2, Risk Management Framework for Information Systems and Organizations: A System Life Cycle Approach for Security and Privacy, https://doi.org/10.6028/NIST.SP.800-37r2

12. NIST SP 800-39, Managing Information Security Risk: Organization, Mission, and Information System View, https://doi.org/10.6028/NIST.SP.800-39

13. NIST SP 800-46, Revision 2, Guide to Enterprise Telework, Remote Access, and Bring Your Own Device (BYOD) Security, https://doi.org/10.6028/NIST.SP.800-46r2

14. NIST SP 800-53, Revision 5 (draft), Security and Privacy Controls for Information Systems and Organizations, https://csrc.nist.gov/publications/detail/sp/800-53/rev-5/draft

15. NIST SP 800-53A, Revision 4, Assessing Security and Privacy Controls in Federal Information Systems and Organizations: Building Effective Assessment Plans, https://doi.org/10.6028/NIST.SP.800-53Ar4

16. NIST SP 800-61, Revision 2, Computer Security Incident Handling Guide, https://doi.org/10.6028/NIST.SP.800-61r2

17. NIST SP 800-63-3, Digital Identity Guidelines, https://doi.org/10.6028/NIST.SP.800-63-3

18. NIST SP 800-77, Guide to IPsec VPNs, https://doi.org/10.6028/NIST.SP.800-77

19. NIST SP 800-84, Guide to Test, Training, and Exercise Programs for IT Plans and Capabilities, https://doi.org/10.6028/NIST.SP.800-84

20. NIST SP 800-88, Revision 1, Guidelines for Media Sanitization, https://doi.org/10.6028/NIST.SP.800-88r1

21. NIST SP 800-113, Guide to SSL VPNs, https://doi.org/10.6028/NIST.SP.800-113

22. NIST SP 800-114, Revision 1, User's Guide to Telework and Bring Your Own Device (BYOD) Security, https://doi.org/10.6028/NIST.SP.800-114r1

23. NIST SP 800-121, Revision 2, Guide to Bluetooth Security, https://doi.org/10.6028/NIST.SP.800-121r2

24. NIST SP 800-160, Volume 1, Systems Security Engineering: Considerations for a Multidisciplinary Approach in the Engineering of Trustworthy Secure Systems, https://doi.org/10.6028/NIST.SP.800-160v1

25. NIST SP 800-161, Supply Chain Risk Management Practices for Federal Information Systems and Organizations, https://doi.org/10.6028/NIST.SP.800-161

26. NIST SP 800-162, Guide to Attribute Based Access Control (ABAC) Definition and Considerations, https://doi.org/10.6028/NIST.SP.800-162

27. NIST SP 800-175B, Guideline for Using Cryptographic Standards in the Federal Government: Cryptographic Mechanisms, https://doi.org/10.6028/NIST.SP.800-175B

28. NIST SP 800-188, De-Identifying Government Datasets (draft), https://csrc.nist.gov/CSRC/media/Publications/sp/800-188/draft/documents/sp800_188_draft2.pdf