From: Michael Pflug <Michael.Pflug@sas.com>
Sent: Thursday, October 24, 2019 1:08 PM
To: privacyframework <privacyframework@nist.gov>
Cc: Cathy Smith <Cathy.Smith@sas.com>
Subject: NIST Privacy Framework: Preliminary Draft Comments

Thank you for the opportunity to review and comment on the preliminary draft of NIST privacy standards. We are pleased to provide the attached feedback and look forward to future iterations of the framework.

Thank you,

Michael Pflug

Advisory Architect, Government and Healthcare

Cell: 734-545-4032

michael.pflug@sas.com

NIST Privacy Framework Preliminary Draft Core

Shading Key: The Function, Category, or Subcategory aligns with the Cybersecurity Framework, but the text has been adapted for the Privacy
The Category or Subcategory is identical to the Cybersecurity Framework.

Function	Category	Subcategory	SAS Comments
IDENTIFY-P (ID-P): Develop the organization-al under-standing 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.	*Please further define "Inventoried" with baseline requirements via Guidance*
		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.	*Please further define "Inventoried" with baseline requirements via Guidance*
		ID.IM-P3: Categories of individuals (e.g., customers, employees or prospective employees, consumers) whose data are being processed are inventoried.	*Please further define "Inventoried" with baseline requirements via Guidance*
		ID.IM-P4: Data actions of the systems/products/services are inventoried.	*Define what "data actions" means.*
		ID.IM-P5: The purposes for the data actions are inventoried.	*This should make a controller/processor distinction.*
		ID.IM-P6: Data elements within the data actions are inventoried.	*This should make a controller/processor distinction.*
		ID.IM-P7: The data processing environment is identified (e.g., geographic location, internal, cloud, third parties).	
		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.	*This should make a controller/processor distinction.* *Templates/clarification of what constitutes an adequate mapping would be useful Guidance.*
	Business Environment (ID.BE-P): The organization's mission, objectives, stakeholders, and activities are	**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.	*Please add details/guidance as this seems vague*
		ID.BE-P3: Systems/products/services that support organizational priorities are identified and key requirements communicated.	
	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,	**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).	*This should make a controller/processor distinction*
		ID.RA-P2: Data analytic inputs and outputs are identified and evaluated for bias.	*Does this responsibility lie with the customer/controller? Model builders?*
		ID.RA-P3: Potential problematic data actions and associated problems are identified.	*Please advise with a controller/processor distinction; the expectations of the two should not be identical.*
		ID.RA-P4: Problematic data actions, likelihoods, and impacts are used to determine and prioritize risk.	*Please advise with a controller/processor distinction; the expectations of the two should not be identical.*
		ID.RA-P5: Risk responses are identified, prioritized, and implemented.	*Please advise with a controller/processor distinction; the expectations of the two should not be identical.*

	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	**ID.DE-P1:** Data processing ecosystem risk management processes are identified, established, assessed, managed, and agreed to by organizational stakeholders.	*Meaningful separation of the privacy elements of these controls from security elements of them would be important to implementing this properly. When can or can't an organization rely on existing security controls to cover privacy risks?*
		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.	*Core elements of a useful privacy risk assessment process should be identified.*
		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 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	**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.	
		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.	*Please add details/guidance as this seems vague. Are these people with "privacy" in their titles only?*
		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.	*Guidance as to what baseline/appropriate policies, processes, and procedures for privacy risks is useful*
	Risk Management Strategy (GV.RM-P): The organization's priorities, constraints, risk tolerances, and	**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	**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.	*What is the scope of what's considered "privacy personnel?"*
		GV.AT-P4: Third parties (e.g., service providers, customers, partners) understand their roles and responsibilities.	
	Monitoring and Review (GV.MT-P): The policies, processes, and procedures for	**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, policies, and training are reviewed and any updates are communicated.	

		ongoing review of the organization's privacy posture are understood and inform the management of privacy risk.	**GV.MT-P3**: Policies, processes, and procedures for assessing compliance with legal requirements and privacy policies are established and in place.	*Please include a processor/controller distinction.*
			GV.MT-P4: Policies, processes, and procedures for communicating progress on managing privacy risks are established and in place.	*Please include a processor/controller distinction.*
			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.,	**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.	*Please include a processor/controller distinction.*
			CT.PO-P2: Policies, processes, and procedures for enabling data review, transfer, sharing 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	**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.	
			CT.DM-P8: Audit/log records are determined, documented, implemented, and reviewed in accordance with policy and incorporating the principle of data minimization.	
		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	**CT.DP-P1:** Data are processed in an unobservable or unlinkable manner (e.g., data actions take place on local devices, privacy-preserving cryptography).	
			CT.DP-P2: Data are processed to limit the identification of individuals (e.g., differential privacy techniques, tokenization).	
			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).	
			CT.DP-P4: System or device configurations permit selective collection or disclosure of data elements.	
			CT.DP-P5: Attribute references are substituted for attribute values.	
			CT.DP-P6: Data processing is limited to that which is relevant and necessary for a system/product/service to meet mission/business objectives.	
	COMMUNICATE-P (CM-P): Develop and implement appropriate activities	**Communication Policies, Processes, and Procedures (CM.PP-P):** Policies,	**CM.PP-P1:** Transparency policies, processes, and procedures for communicating data processing purposes, practices, and associated privacy risks are established and in place.	
			CM.PP-P2: Roles and responsibilities (e.g., public relations) for communicating data processing purposes, practices, and associated privacy risks are established.	

to enable organizations and individuals to have a reliable understanding about how data are processed and associated privacy risks.	**Data Processing Awareness (CM.AW-P):** 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.	**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.	
		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.	
		CM.AW-P3: System/product/service design enables data processing visibility.	
		CM.AW-P4: Records of data disclosures and sharing are maintained and can be accessed for review or transmission/disclosure.	
		CM.AW-P5: Data corrections or deletions can be communicated to individuals or organizations (e.g., data sources) in the data processing ecosystem.	
		CM.AW-P6: Data provenance and lineage are maintained and can be accessed for review or transmission/disclosure.	
		CM.AW-P7: Impacted individuals and organizations are notified about a privacy breach or event.	
		CM.AW-P8: Individuals are provided with mitigation mechanisms to address impacts to individuals that arise from data processing.	*Please provide guidance - could this include things like credit monitoring?*
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	**PR.AC-P1:** Identities and credentials are issued, managed, verified, revoked, and audited for authorized individuals, processes, and devices.	
		PR.AC-P2: Physical access to data and devices is managed.	
		PR.AC-P3: Remote access is managed.	
		PR.AC-P4: Access permissions and authorizations are managed, incorporating the principles of least privilege and separation of duties.	
		PR.AC-P5: Network integrity is protected (e.g., network segregation, network segmentation).	
		PR.AC-P6: Individuals and devices are proofed and bound to credentials, and authenticated commensurate with the risk of the transaction (e.g., individuals' 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.	
		PR.DS-P2: Data-in-transit are protected.	
		PR.DS-P3: Systems/products/services and associated data are formally managed throughout removal, transfers, and disposition.	
		PR.DS-P4: Adequate capacity to ensure availability is maintained.	
		PR.DS-P5: Protections against data leaks are implemented.	
		PR.DS-P6: Integrity checking mechanisms are used to verify software, firmware, and information integrity.	
		PR.DS-P7: The development and testing environment(s) are separate from the production environment.	
		PR.DS-P8: Integrity checking mechanisms are used to verify hardware integrity.	
	Data Protection Policies, Processes, and Procedures (PR.DP-P): Security and privacy policies (which address purpose, scope, roles, responsibilities, management commitment, and	**PR.DP-P1:** A baseline configuration of information technology is created and maintained incorporating security principles (e.g., concept of least functionality).	
		PR.DP-P2: Configuration change control processes are established and in place.	
		PR.DP-P3: Backups of information are conducted, maintained, and tested.	
		PR.DP-P4: Policy and regulations regarding the physical operating environment for organizational assets are met.	
		PR.DP-P5: Protection processes are improved.	
		PR.DP-P6: Effectiveness of protection technologies is shared.	
		PR.DP-P7: Response plans (Incident Response and Business Continuity) and recovery plans (Incident Recovery and Disaster Recovery) are established, in place, and managed.	

	coordination among organizational entities), processes, and procedures are	**PR.DP-P8:** Response and recovery plans are tested.	
		PR.DP-P9: Privacy procedures are included in human resources practices (e.g., deprovisioning, personnel screening).	
		PR.DP-P10: A vulnerability management plan is developed and implemented.	
	Maintenance (PR.MA-P): System maintenance and repairs are performed	**PR.MA-P1:** Maintenance and repair of organizational assets are 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.	
	Protective Technology (PR.PT-P): Technical security solutions are managed to ensure the security and resilience of systems/products/serv	**PR.PT-P1:** Removable media is protected and its use restricted according to policy.	
		PR.PT-P2: The principle of least functionality is incorporated by configuring systems to provide only essential capabilities.	
		PR.PT-P3: Communications and control networks are protected.	*Please provide guidance as this is a bit vague*
		PR.PT-P4: Mechanisms (e.g., failsafe, load balancing, hot swap) are implemented to achieve resilience requirements in normal and adverse situations.	