DRAFT - OCTOBER 19

November 4, 2023

VIA EMAIL: cyberframework@nist.gov

Cybersecurity Framework
National Institute of Standards and Technology
100 Bureau Drive, Stop 2000
Gaithersburg, MD 20899

Re: Discussion Draft of the NIST Cybersecurity Framework 2.0 Core with Implementation Examples

The Cybersecurity Coalition (the Coalition) submits the following comments in response to the National Institute for Standards and Technology (NIST) Discussion Draft of the Cybersecurity Framework (CSF) 2.0 Core with Implementation Examples.[1] The Coalition appreciates the opportunity to provide input, and we commend NIST for its openness and commitment to working with industry stakeholders to address the updates to the CSF.

The Coalition is composed of leading companies with a specialty in cybersecurity products and services, who are dedicated to finding and advancing consensus policy solutions that promote the development and adoption of cybersecurity technologies.[2] We seek to ensure a robust marketplace and effective policy environment that will encourage companies of all sizes to take steps to improve cybersecurity risk management.

The Coalition is broadly supportive of the proposed changes to the CSF Core. Echoing our previous comments on updates to the CSF 2.0 Core, the Coalition was pleased to see the addition of the Governance function; the reorganizing of categories and subcategories to follow a pre-incident and post-incident chronology; the removal of references to critical infrastructure;

[1] NIST Cyberscurity Framework 2.0, Aug. 8, 2023, https://csrc.nist.gov/pubs/cswp/29/the-nist-cybersecurity-framework-20/ipd.
[2] Cybersecurity Coalition, https://www.cybersecuritycoalition.org, (last accessed Oct. 17, 2023).

the inclusion of a traceability matrix and implementation examples; and increased engagement with international partners.[3] Additionally, the Coalition would like to offer further recommendations on the following topic areas:

1. **Consistency between CSF and Privacy Framework**

The Coalition underscores the importance of ensuring alignment between the CSF 2.0 Core and the Privacy Framework.[4] The Coalition has long been supportive of a risk-based Privacy Framework that incorporates effective security principles to enable consistent risk management across both privacy and data security.[5]

Many organizations are already using, or may be planning to use, the CSF in conjunction with the Privacy Framework to jointly address privacy and cybersecurity risks. To avoid misalignment, it is important that the Privacy Framework reflects changes being made in the CSF. Given that the NIST Privacy Framework leverages CSF functions, categories, and subcategories, especially in the Protect-P function, the Coalition does not believe this should require a major revision to the Privacy Framework, but could be accomplished through a minor update (e.g., a version 1.1).

To help facilitate these updates, the Coalition offers an Appendix to these comments that includes a mapping of the Privacy Framework, CSF v1.1, and CSF 2.0 Core.[6] This mapping expands on the current NIST crosswalk between the CSF v1.1 and Privacy Framework[7] with an additional column for the CSF 2.0 Core updates, noting where NIST may wish to consider updates in the Privacy Framework (especially in the Protect function).

Going forward, we suggest NIST consider an update cadence for the CSF and the Privacy Framework that minimizes periods of inconsistency between the two documents.

---

[3] Cybersecurity Coalition, Comments on the NIST Cybersecurity Framework 2.0 Core Discussion Draft, May 29, 2023, https://www.cybersecuritycoalition.org/filings/coalition-comments-on-nist-cybersecurity-framework-2-0-core-discussion-draft.

[4] NIST, Privacy Framework, Jan. 16, 2020, https://www.nist.gov/privacy-framework.

[5] Cybersecurity Coalition, Request for Information Response to NIST Regarding "Developing a Privacy Framework", Jan. 14, 2019, https://www.cybersecuritycoalition.org/filings/request-for-information-response-to-the-national-institute-of-standards-and-technology-nist-regarding-developing-a-privacy-framework.

[6] See Appendix A. See also, Jamie Danker, Cybersecurity Coalition, Crosswalk Resource - NIST Privacy Framework to Cybersecurity Framework 1.1 and DRAFT CSF 2.0 2023, available at https://docs.google.com/spreadsheets/d/1etLMEs4rGFsRayIpFfW9netq6Qi8Wme2X9GM3OxhQvU/edit#gid=1864081823.

[7] NIST, Cybersecurity Framework Crosswalk, Jan. 16, 2020, https://www.nist.gov/privacy-framework/resource-repository/browse/crosswalks/cybersecurity-framework-crosswalk.

2. Practical Guidance Needed on Utilizing Multiple NIST Risk Management Frameworks

The Coalition also suggests that NIST publish resources regarding how the different risk management frameworks align with one another, and how stakeholders can use multiple frameworks together in a practical way. NIST currently offers a variety of frameworks for organizations to measure and manage their cybersecurity risk including the CSF 2.0, the Privacy Framework, the Risk Management Framework (RMF),[8] the Cybersecurity Supply Chain Risk Management (C-SCRM),[9] and most recently, the Artificial Intelligence Risk Management Framework (AI RMF).[10] Many organizations would benefit from leveraging multiple frameworks, and NIST should aim to streamline this activity.

We acknowledge that NIST has made efforts to relate the CSF to other frameworks and resources in the draft CSF 2.0 Core. Going forward, as NIST updates these risk management frameworks, we suggest developing them in a way that achieves structural alignment. This should include, for example, consistent phrasing for Functions, Categories, and Subcategories whenever feasible.

NIST should consider leveraging the National Cybersecurity Center of Excellence (NCCOE) to produce further guidance on how NIST publications can work in tandem, where they diverge, and how to practically implement multiple frameworks.

3. Simplify Online Tools for Informative References

The Coalition would like to reiterate our previous comments and encourage NIST to explore ways to provide online tools for informative references that meet the needs and capabilities of the entire community using the CSF.[11] The NIST Cybersecurity and Privacy Tool (CPRT)[12] and the Online Informative References Program (OLIR)[13] Catalogs are complex tools that could pose a barrier to CSF users who are unfamiliar with these tools. As NIST transitions to these dynamic

[8] NIST, Risk Management Framework, https://csrc.nist.gov/projects/risk-management/about-rmf (Last accessed Oct. 18, 2023).
[9] NIST, Cybersecurity Supply Chain Risk Management, May 24, 2016, https://csrc.nist.gov/projects/cyber-supply-chain-risk-management.
[10] NIST, AI Risk Management Framework, Jul. 28, 2021, https://www.nist.gov/itl/ai-risk-management-framework/ai-rmf-development.
[11] Cybersecurity Coalition, Coalition Comments on NIST Cybersecurity Framework 2.0 Core Discussion Draft, May 29, 2023, www.cybersecuritycoalition.org/filings/coalition-comments-on-nist-cybersecurity-framework-2-0-core-discussion-draft.
[12] NIST, Cybersecurity and Privacy Reference Tool (CPRT), Mar. 3, 2022, https://csrc.nist.gov/Projects/cprt.
[13] NIST, National Online Informative References (OLIR) Program, Sep. 8, 2020, https://csrc.nist.gov/Projects/olir.

tools, it is critical to ensure that they are as usable as having a set of informative references directly in the Framework document. Presently they are not.

The Coalition is also aware of the new Cybersecurity Framework Reference Tool[14] that is intended to allow users to explore the different functions, categories, subcategories, and implementation examples of the CSF. While we are supportive of the intended use of the tool, the addition of this tool adds to the complexity of navigating the many resources published by NIST. Currently, it is not clear how the Cybersecurity Framework Reference Tool operates in relation to the CPRT and OLIR. One of the fundamental reasons for updating the CSF was due to the number of small- and medium-sized entities that have used the framework for their cybersecurity risk management practices. Therefore, the resources created for understanding and implementing the CSF must accommodate organizations of all sizes and maturity levels. The organizations that stand to benefit the most from using the CSF will need to have this complexity managed for them.

Going forward, NIST should prioritize the usability of its resources, make clear the full array of resources available, how to access them, how they are different, and what their specific use cases are. The Coalition also wishes to know whether there will be a feedback period of the new tool, and if NIST is engaging with a wide variety of users during the development of this tool.

Historically, organizations have based their cyber risk management on a specific set of international standards or industry best practices. Many compliance teams in industries that are regulated under multiple authorities have to compare the requirements of multiple standards. Ideally, NIST would develop a resource that enabled a user to generate a self-contained and customized document that maps multiple standards and best practice documents they identify as being relevant to their organization. This tool would allow for discreet use cases such as mapping a single function to a standard/framework, as well as the ability to crosswalk multiple standards or frameworks. Users would generate a copy of the CSF 2.0 (or other NIST risk management framework) with the informative references section filled in with the user-selected set of mapped references. A new version could be regenerated when a new or updated applicable standard or best practice document was added to the online references tool. We believe this would best satisfy the global community of stakeholders by making the CSF (or other related NIST framework documents) more readily consumable in a manner customized to be more relevant to the needs of the individual organization.

[14] NIST, Cybersecurity Framework, https://csrc.nist.gov/Projects/cybersecurity-framework/Filters#/csf/filters (last accessed Oct. 18, 2023).

* * *

The Coalition appreciates that NIST continually listens to the private sector and thanks NIST for allowing us to contribute our thoughts and recommendations to the dialog. As the conversation around this topic continues to evolve, we would welcome the opportunity to further serve as a resource on both technical and policy questions to ensure that Cybersecurity Framework continues to be successful in driving consistent, effective cyber risk management practices globally.

Respectfully submitted,

The Cybersecurity Coalition

Crosswalk from the NIST Privacy Framework Core to the Framework for Improving Critical Infrastructure Cybersecurity V1.1 and DRAFT NIST Cybersecurity Framework 2.0 Core

NIST Privacy Framework Core			Cybersecurity Framework Subcategory V 1.1	Cybersecurity Framework Subcategory DRAFT 2.0
Function	Category	Subcategory		
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.	**ID.AM-1:** Physical devices and systems within the organization are inventoried **ID.AM-2:** Software platforms and applications within the organization are inventoried	**ID.AM-01:** Inventories of hardware managed by the organization are maintained **ID.AM-02:** Inventories of software, services, and systems managed by the organization are maintained
		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.	**ID.AM-1:** Physical devices and systems within the organization are inventoried **ID.AM-4:** External information systems are catalogued	**ID.AM-01:** Inventories of hardware managed by the organization are maintained **ID.AM-02:** Inventories of software, services, and systems managed by the organization are maintained **ID.AM-04:** Inventories of services provided by suppliers are maintained
		ID.IM-P3: Categories of individuals (e.g., customers, employees or prospective employees, consumers) 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.AM-07**: Inventories of data and corresponding metadata for designated data types are maintained
		ID.IM-P7: The data processing environment is identified (e.g., geographic location, internal, cloud, third parties).	**ID.AM-1:** Physical devices and systems within the organization are inventoried **ID.AM-2:** Software platforms and applications within the organization are inventoried **ID.AM-4:** External information systems are catalogued	**ID.AM-01**: Inventories of hardware managed by the organization are maintained **ID.AM-02:** Inventories of software, services, and systems managed by the organization are maintained **ID.AM-04:** Inventories of services provided by suppliers are maintained
		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.	**ID.AM-3:** Organizational communication and data flows are mapped	**ID.AM-03**: Representations of the organization's authorized network communication and internal and external network data flows are maintained
	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(s) in the data processing ecosystem are identified and communicated.	**ID.BE-1:** The organization's role in the supply chain is identified and communicated	**GV.OC-05:** Outcomes, capabilities, and services that the organization depends on are determined and communicated
		ID.BE-P2: Priorities for organizational mission, objectives, and activities are established and communicated.	**ID.BE-3:** Priorities for organizational mission, objectives, and activities are established and communicated.	**GV.OC-01:** The organizational mission is understood and informs cybersecurity risk management **GV.OC-04:** Critical objectives, capabilities, and services that stakeholders depend on or expect from the organization are determined and communicated
		ID.BE-P3: Systems/products/services that support organizational priorities are identified and key requirements communicated.		**GV.OC-04:** Critical objectives, capabilities, and services that stakeholders depend on or expect from the organization are determined and communicated **GV.OC-05:** Outcomes, capabilities, and services that the organization depends on are determined and 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, 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 and/or types, visibility of data processing to individuals and third parties).		
		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-4:** Potential business impacts and likelihoods are identified **ID.RA-5:** Threats, vulnerabilities, likelihoods, and impacts are used to determine risk	**ID.RA-04:** Potential impacts and likelihoods of threats exploiting vulnerabilities are identified and recorded **ID.RA-05:** Threats, vulnerabilities, likelihoods, and impacts are used to determine risk and inform risk prioritization
		ID.RA-P5: Risk responses are identified, prioritized, and implemented.	**ID.RA-6:** Risk responses are identified and prioritized	**ID.RA-06:** Risk responses are chosen from the available options, prioritized, planned, tracked, and communicated
	Data Processing Ecosystem Risk Management (ID.DE-P): The organization's priorities, constraints, risk tolerance, 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 policies, processes, and procedures are identified, established, assessed, managed, and agreed to by organizational stakeholders.	**ID.SC-1:** Cyber supply chain risk management processes are identified, established, assessed, managed, and agreed to by organizational stakeholders	**GV.SC-01:** A cybersecurity supply chain risk management program, strategy, objectives, policies, and processes are established and agreed to by organizational stakeholders **GV.SC-02:** Cybersecurity roles and responsibilities for suppliers,
		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.SC-2:** Suppliers and third-party partners of information systems, components, and services are identified, prioritized, and assessed using a cyber supply chain risk assessment process	**GV.SC-03:** Cybersecurity supply chain risk management is integrated into cybersecurity and enterprise risk management, risk assessment, and improvement processes
		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.SC-3:** Contracts with suppliers and third-party partners are used to implement appropriate measures designed to meet the objectives of an organization's cybersecurity program and Cyber Supply Chain Risk Management Plan.	**GV.SC-05**: Requirements to address cybersecurity risks in supply chains are established, prioritized, and integrated into contracts and other types of agreements with suppliers and other relevant third parties
		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, interoperability framework, or other obligations.	**ID.SC-4:** Suppliers and third-party partners are routinely assessed using audits, test results, or other forms of evaluations to confirm they are meeting their contractual obligations.	**GV.SC-07**: The risks posed by a supplier, their products and services, and other third parties are identified, recorded, prioritized, assessed, responded to, and monitored over the course of the relationship
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.PO-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.PO-P1:** Organizational privacy values and policies (e.g., conditions on data processing such as data uses or retention periods, individuals' prerogatives with respect to data processing) are established and communicated.	**ID.GV-1:** Organizational cybersecurity policy is established and communicated	**GV.PO-01:** Policies, processes, and procedures for managing cybersecurity risks are established based on organizational context, cybersecurity strategy, and priorities and are communicated and enforced
		GV.PO-P2: Processes to instill organizational privacy values within system/product/service development and operations are established and in place.		**GV.PO-01:** Policies, processes, and procedures for managing cybersecurity risks are established based on organizational context, cybersecurity strategy, and priorities and are communicated and enforced
		GV.PO-P3: Roles and responsibilities for the workforce are established with respect to privacy.	**ID.AM-6:** Cybersecurity roles and responsibilities for the entire workforce and third-party stakeholders (e.g., suppliers, customers, partners) are established	**GV.SC-02**: Cybersecurity roles and responsibilities for suppliers, customers, and partners are established, communicated, and coordinated internally and externally

Shading Key:

The Function, Category, or Subcategory is identical to the Cybersecurity Framework.

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

		GV.PO-P4: Privacy roles and responsibilities are coordinated and aligned with third-party stakeholders (e.g., service providers, customers, partners).	**ID.GV-2:** Cybersecurity roles and responsibilities are coordinated and aligned with internal roles and external partners	**GV.SC-02:** Cybersecurity roles and responsibilities for suppliers, customers, and partners are established, communicated, and coordinated internally and externally
		GV.PO-P5: Legal, regulatory, and contractual requirements regarding privacy are understood and managed.	**ID.GV-3:** Legal and regulatory requirements regarding cybersecurity, including privacy and civil liberties obligations, are understood and managed	**GV.OC-03**: Legal, regulatory, and contractual requirements regarding cybersecurity — including privacy and civil liberties obligations — are understood and managed
		GV.PO-P6: Governance and risk management policies, processes, and procedures address privacy risks.	**ID.GV-4:** Governance and risk management processes address cybersecurity risks	**GV.RM-03:** Enterprise risk management processes include cybersecurity risk management activities and outcomes
	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.	**ID.RM-1:** Risk management processes are established, managed, and agreed to by organizational stakeholders	**GV.RM-01**: Risk management objectives are established and agreed to by organizational stakeholders
		GV.RM-P2: Organizational risk tolerance is determined and clearly expressed.	**ID.RM-2:** Organizational risk tolerance is determined and clearly expressed	**GV.RM-02**: Risk appetite and risk tolerance statements are determined, communicated, and maintained
		GV.RM-P3: The organization's determination of risk tolerance is informed by its role(s) in the data processing ecosystem.	**ID.RM-3:** The organization's determination of risk tolerance is informed by its role in critical infrastructure and sector specific risk analysis	**GV.RM-02:** Risk appetite and risk tolerance statements are determined, communicated, and maintained
	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.	**PR.AT-1:** All users are informed and trained **PR.AT-2:** Privileged users understand their roles and responsibilities	**PR.AT-01**: Users are provided awareness and training so they possess the knowledge and skills to perform general tasks with security risks in mind
		GV.AT-P2: Senior executives understand their roles and responsibilities.	**PR.AT-4:** Senior executives understand their roles and responsibilities	**PR.AT-02**: Individuals in specialized roles are provided awareness and training so they possess the knowledge and skills to perform relevant tasks with security risks in mind
		GV.AT-P3: Privacy personnel understand their roles and responsibilities.	**PR.AT-5:** Physical and cybersecurity personnel understand their roles and responsibilities	**PR.AT-01:** Users are provided awareness and training so they possess the knowledge and skills to perform general tasks with
		GV.AT-P4: Third parties (e.g., service providers, customers, partners) understand their roles and responsibilities.	**PR.AT-3:** Third-party stakeholders (e.g., suppliers, customers, partners) understand their roles and responsibilities	**PR.AT-01**: Users are provided awareness and training so they possess the knowledge and skills to perform general tasks with security risks in mind **PR.AT-02**: Individuals in specialized roles are provided awareness and training so they possess the knowledge and skills to perform relevant tasks with security risks in mind
	Monitoring and Review (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 (e.g., introduction of new technologies), governance (e.g., legal obligations, risk tolerance), data processing, and systems/products/services change.		**GV.PO-02:** Policies, processes, and procedures for managing cybersecurity risks are reviewed, updated, communicated, and enforced to reflect changes in requirements, threats, technology, and organizational mission
		GV.MT-P2: Privacy values, policies, and training are reviewed and any updates are communicated.		**GV.PO-02:** Policies, processes, and procedures for managing cybersecurity risks are reviewed, updated, communicated, and
		GV.MT-P3: Policies, processes, and procedures for assessing compliance with legal requirements and privacy policies are established and in place.		
		GV.MT-P4: Policies, processes, and procedures for communicating progress on managing privacy risks are established and in place.		**GV.OV-03:** Organizational cybersecurity risk management performance is measured and reviewed to confirm and adjust strategic direction
		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, professional events).		
		GV.MT-P6: Policies, processes, and procedures incorporate lessons learned from problematic data actions.		**ID.IM-03**: Lessons learned during execution of operational processes, procedures, and activities are used to identify improvements
		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 Processing Policies, Processes, and Procedures (CT.PO-P):** Policies, processes, and procedures are maintained and used to manage data processing (e.g., purpose, scope, roles and responsibilities in the data processing ecosystem, and management commitment) 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, transfer, sharing or disclosure, alteration, and deletion are established and in place (e.g., to maintain data quality, manage data retention).		
		CT.PO-P3: Policies, processes, and procedures for enabling individuals' data processing preferences and requests are established and in place.		
		CT.PO-P4: A data life cycle to manage data is aligned and implemented with the system development life cycle to manage systems.	**PR.IP-2:** A system development life cycle to manage systems is implemented	**ID.AM-08**: Systems, hardware, software, and services are managed throughout their life cycle
	Data Processing 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.	**PR.IP-6**: Data is destroyed according to policy	**PR.DS-09:** Data is managed throughout its life cycle, including destruction
		CT.DM-P6: Data are transmitted using standardized		
		CT.DM-P7: Mechanisms for transmitting processing permissions and related data values with data elements are established and in place.		
		CT.DM-P8: Audit/log records are determined, documented, implemented, and reviewed in accordance with policy and incorporating the principle of data minimization.	**PR.PT-1:** Audit/log records are determined, documented, implemented, and reviewed in accordance with policy	**PR.PS-04:** Log records are generated and made available for continuous monitoring
		CT.DM-P9: Technical measures implemented to manage data processing are tested and assessed.		
		CT.DM-P10: Stakeholder privacy preferences are included in algorithmic design objectives and outputs are evaluated against these preferences.		
	Disassociated Processing (CT.DP-P): Data processing solutions increase disassociability consistent with the organization's risk strategy to protect individuals' privacy and enable implementation of privacy principles (e.g., data minimization).	**CT.DP-P1:** Data are processed to limit observability and linkability (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., de-identification privacy techniques, tokenization).		
		CT.DP-P3: Data are processed to limit 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.		
COMMUNICATE-P (CM-P): Develop and implement appropriate activities to enable organizations and individuals to have a reliable understanding and engage in a dialogue about how data are processed and associated privacy risks.	**Communication Policies, Processes, and Procedures (CM.PO-P):** Policies, processes, and procedures are maintained and used to increase transparency of the organization's data processing practices (e.g., purpose, scope, roles and responsibilities in the data processing ecosystem, and management commitment) and associated privacy risks.	**CM.PO-P1:** Transparency policies, processes, and procedures for communicating data processing purposes, practices, and associated privacy risks are established and in place.		
		CM.PO-P2: Roles and responsibilities (e.g., public relations) for communicating data processing purposes, practices, and associated privacy risks are established.		
	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 (e.g., credit monitoring, consent withdrawal, data alteration or deletion) to address impacts of problematic data actions.		
PROTECT-P (PR-P): Develop and implement appropriate data processing safeguards.	**Data Protection Policies, Processes, and Procedures (PR.PO-P)**: Security and privacy policies (e.g., purpose, scope, roles and responsibilities in the data processing ecosystem, and management commitment), processes, and procedures are maintained and used to manage the protection of data.	**PR.PO-P1**: A baseline configuration of information technology is created and maintained incorporating security principles (e.g., concept of least functionality).	**PR.IP-1**: A baseline configuration of information technology/industrial control systems is created and maintained incorporating security principles (e.g. concept of least functionality)	**PR.PS-01**: Configuration management practices are applied
		PR.PO-P2: Configuration change control processes are established and in place.	**PR.IP-3:** Configuration change control processes are in place	**ID.AM-08:** Systems, hardware, software, and services are managed throughout their life cycle
		PR.PO-P3: Backups of information are conducted, maintained, and tested.	**PR.IP-4:** Backups of information are conducted, maintained, and tested	**PR.PS-01:** Configuration management practices are applied **ID.RA-07:** Changes and exceptions are managed, assessed for risk impact, recorded, and tracked
		PR.PO-P4: Policy and regulations regarding the physical operating environment for organizational assets are met.	**PR.IP-5:** Policy and regulations regarding the physical operating environment for organizational assets are met	**PR.IR-02:** The organization's technology assets are protected from environmental threats
		PR.PO-P5: Protection processes are improved.	**PR.IP-7:** Protection processes are improved	**ID.IM-03:** Lessons learned during execution of operational processes, procedures, and activities are used to identify improvements
		PR.PO-P6: Effectiveness of protection technologies is shared.	**PR.IP-8:** Effectiveness of protection technologies is shared	**ID.IM-03:** Lessons learned during execution of operational processes, procedures, and activities are used to identify improvements
		PR.PO-P7: Response plans (Incident Response and Business Continuity) and recovery plans (Incident Recovery and Disaster Recovery) are established, in place, and managed.	**PR.IP-9:** Response plans (Incident Response and Business Continuity) and recovery plans (Incident Recovery and Disaster Recovery) are in place and managed	**ID.IM-04:** Cybersecurity plans that affect operations are communicated, maintained, and improved
		PR.PO-P8: Response and recovery plans are tested.	**PR.IP-10:** Response and recovery plans are tested	**ID.IM-02:** Security tests and exercises, including those done in coordination with suppliers and relevant third parties, are conducted to identify improvements
		PR.PO-P9: Privacy procedures are included in human resources practices (e.g., deprovisioning, personnel screening).	**PR.IP-11:** Cybersecurity is included in human resources practices (e.g., deprovisioning, personnel screening)	**GV.RR-04:** Cybersecurity is included in human resources practices
		PR.PO-P10: A vulnerability management plan is developed and implemented.	**PR.IP-12:** A vulnerability management plan is developed and implemented	**ID.RA-01:** Vulnerabilities in assets are identified, validated, and recorded **PR.PS-02:** Software is maintained, replaced, and removed commensurate with risk
	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.	**PR.AC-1:** Identities and credentials are issued, managed, verified, revoked, and audited for authorized devices, users and processes	**PR.AA-01:** Identities and credentials for authorized users, services, and hardware are managed by the organization **PR.AA-05:** Access permissions, entitlements, and authorizations are defined in a policy, managed, enforced, and reviewed, and incorporate the principles of least privilege and separation of duties
		PR.AC-P2: Physical access to data and devices is managed.	**PR.AC-2:** Physical access to assets is managed and protected	**PR.AA-06**: Physical access to assets is managed, monitored, and enforced commensurate with risk
		PR.AC-P3: Remote access is managed.	**PR.AC-3:** Remote access is managed	**PR.AA-03**: Users, services, and hardware are authenticated **PR.AA-05:** Access permissions, entitlements, and authorizations are defined in a policy, managed, enforced, and reviewed, and incorporate the principles of least privilege and separation of duties **PR.IR-01:** Networks and environments are protected from unauthorized logical access and usage
		PR.AC-P4: Access permissions and authorizations are managed, incorporating the principles of least privilege and separation of duties.	**PR.AC-4:** Access permissions and authorizations are managed, incorporating the principles of least privilege and separation of duties	**PR.AA-05:** Access permissions, entitlements, and authorizations are defined in a policy, managed, enforced, and reviewed, and incorporate the principles of least privilege and separation of duties
		PR.AC-P5: Network integrity is protected (e.g., network segregation, network segmentation).	**PR.AC-5:** Network integrity is protected (e.g., network segregation, network segmentation)	**PR.IR-01:** Networks and environments are protected from unauthorized logical access and usage
		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).	**PR.AC-6:** Identities are proofed and bound to credentials and asserted in interactions **PR.AC-7:** Users, devices, and other assets are authenticated (e.g., single-factor, multi-factor) commensurate with the risk of the transaction (e.g., individuals' security and privacy risks and other organizational risks)	**PR.AA-02:** Identities are proofed and bound to credentials based on the context of interactions **PR.AA-03**: Users, services, and hardware are authenticated
	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-1:** Data-at-rest is protected	**PR.DS-01**: The confidentiality, integrity, and availability of data-at-rest are protected
		PR.DS-P2: Data-in-transit are protected.	**PR.DS-2:** Data-in-transit is protected	**PR.DS-02:** The confidentiality, integrity, and availability of data-in-transit are protected
		PR.DS-P3: Systems/products/services and associated data are formally managed throughout removal, transfers, and disposition.	**PR.DS-3:** Assets are formally managed throughout removal, transfers, and disposition	**ID.AM-08:** Systems, hardware, software, and services are managed throughout their life cycle

		PR.DS-P4: Adequate capacity to ensure availability is maintained.	**PR.DS-4:** Adequate capacity to ensure availability is maintained	**PR.IR-04:** Adequate resource capacity to ensure availability is maintained
		PR.DS-P5: Protections against data leaks are implemented.	**PR.DS-5:** Protections against data leaks are implemented	**PR.DS-01:** The confidentiality, integrity, and availability of data-at-rest are protected **PR.DS-02:** The confidentiality, integrity, and availability of data-in-transit are protected **PR.DS-10:** The confidentiality, integrity, and availability of data-in-use are protected
		PR.DS-P6: Integrity checking mechanisms are used to verify software, firmware, and information integrity.	**PR.DS-6:** Integrity checking mechanisms are used to verify software, firmware, and information integrity	**PR.DS-01:** The confidentiality, integrity, and availability of data-at-rest are protected **DE.CM-09:** Computing hardware and software, runtime environments, and their data are monitored to find potentially adverse events
		PR.DS-P7: The development and testing environment(s) are separate from the production	**PR.DS-7:** The development and testing environment(s) are separate from the production environment	**PR.IR-01:** Networks and environments are protected from unauthorized logical access and usage
		PR.DS-P8: Integrity checking mechanisms are used to verify hardware integrity.	**PR.DS-8:** Integrity checking mechanisms are used to verify hardware integrity	**ID.RA-09:** The authenticity and integrity of hardware and software are assessed prior to acquisition and use **DE.CM-09:** Computing hardware and software, runtime environments, and their data are monitored to find potentially adverse events
	Maintenance (PR.MA-P): System maintenance and repairs are performed consistent with policies, processes, and procedures.	**PR.MA-P1:** Maintenance and repair of organizational assets are performed and logged, with approved and controlled tools.	**PR.MA-1:** Maintenance and repair of organizational assets are performed and logged, with approved and controlled tools	**ID.AM-08:** Systems, hardware, software, and services are managed throughout their life cycle **PR.PS-03:** Hardware is maintained, replaced, and removed commensurate with risk
		PR.MA-P2: Remote maintenance of organizational assets is approved, logged, and performed in a manner that prevents unauthorized access.	**PR.MA-2:** Remote maintenance of organizational assets is approved, logged, and performed in a manner that prevents unauthorized access	**ID.AM-08:** Systems, hardware, software, and services are managed throughout their life cycle **PR.PS-02:** Software is maintained, replaced, and removed commensurate with risk
	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.	**PR.PT-2**: Removable media is protected and its use restricted according to policy	**PR.DS-01:** The confidentiality, integrity, and availability of data-at-rest are protected **PR.PS-01:** Configuration management practices are applied
		PR.PT-P2: The principle of least functionality is incorporated by configuring systems to provide only essential capabilities.	**PR.PT-3:** The principle of least functionality is incorporated by configuring systems to provide only essential capabilities	**PR.PS-01**: Configuration management practices are applied
		PR.PT-P3: Communications and control networks are protected.	**PR.PT-4:** Communications and control networks are protected	**PR.IR-01:** Networks and environments are protected from unauthorized logical access and usage
		PR.PT-P4: Mechanisms (e.g., failsafe, load balancing, hot swap) are implemented to achieve resilience requirements in normal and adverse situations.	**PR.PT-5:** Mechanisms (e.g., failsafe, load balancing, hot swap) are implemented to achieve resilience requirements in normal and adverse situations	**PR.IR-03:** Mechanisms are implemented to achieve resilience requirements in normal and adverse situations