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;

---


the inclusion of a traceability matrix and implementation examples; and increased engagement with international partners. 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. 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.

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. This mapping expands on the current NIST crosswalk between the CSF v1.1 and Privacy Framework 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.

---


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/1etLMEs4rGFsRayIpFfW9netq6Qi8Wme2X9GM3OhQvU/edit#gid=1864081823.

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

---


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\textsuperscript{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.

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

<table>
<thead>
<tr>
<th>NIST Privacy Framework Core</th>
<th>Cybersecurity Framework Subcategory V1.1</th>
<th>Cybersecurity Framework Subcategory DRAFT 2.0</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>IDENTIFY-P (ID-P)</strong>: Develop the organizational understanding to manage privacy risk for individuals arising from data processing.</td>
<td><strong>AM-01</strong>: Inventories of hardware managed by the organization are maintained.</td>
<td><strong>AM-02</strong>: Inventories of software, services, and systems managed by the organization are maintained.</td>
</tr>
<tr>
<td><strong>DATA-P1</strong>: Systems/products/services that process data are inventoried.</td>
<td><strong>AM-03</strong>: Inventories of hardware managed by the organization are maintained.</td>
<td><strong>AM-04</strong>: Inventories of software, services, and systems managed by the organization are maintained.</td>
</tr>
<tr>
<td><strong>DATA-P2</strong>: Data elements within the data actions are inventoried.</td>
<td><strong>AM-07</strong>: Inventories of data and corresponding metadata for designated data types are maintained.</td>
<td><strong>AM-05</strong>: Inventories of services provided by suppliers are maintained.</td>
</tr>
<tr>
<td><strong>DATA-P3</strong>: Data processing is mapped, illustrating the data actions and associated data elements for systems/products/services, including components; roles of the component owner/operator, and interactions of individuals or third parties with the systems/products/services.</td>
<td><strong>AM-3</strong>: Organizational communication and data flows are mapped.</td>
<td><strong>AM-3</strong>: Representations of the organization’s software network communication and internal and external network data flows are maintained.</td>
</tr>
<tr>
<td><strong>DATA-P4</strong>: The organization's role(s) in the data processing ecosystem are identified and communicated.</td>
<td><strong>GV-OC-05</strong>: Outcome, capabilities, and services that the organization depends on are determined and communicated.</td>
<td><strong>GV-OC-04</strong>: Critical objectives, capabilities, and services that stakeholders depend on or expect from the organization are determined and communicated.</td>
</tr>
<tr>
<td><strong>DATA-P5</strong>: Data analytic inputs and outputs are identified and evaluated for bias.</td>
<td><strong>GV-SC-07</strong>: Cybersecurity roles and responsibilities for suppliers, customers, and partners are established, prioritized, and integrated into contracts and other types of agreements with suppliers and other relevant third parties.</td>
<td><strong>GV-SC-05</strong>: Cybersecurity supply chain risk management is integrated into cybersecurity and enterprise risk management, risk assessment, and improvement processes.</td>
</tr>
<tr>
<td><strong>DATA-P6</strong>: Potential problematic data actions and associated problems are identified.</td>
<td><strong>GV-SC-03</strong>: Cybersecurity supply chain risk management program; strategy, objectives, policies, and processes are established and agreed to by organizational stakeholders.</td>
<td><strong>GV-SC-01</strong>: Cybersecurity supply chain risk management strategy, objectives, policies, and processes are established and communicated.</td>
</tr>
<tr>
<td><strong>DATA-P7</strong>: 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).</td>
<td><strong>GV-SC-02</strong>: Cybersecurity roles and responsibilities for suppliers, customers, and partners are established, prioritized, and integrated into contracts and other types of agreements with suppliers and other relevant third parties.</td>
<td><strong>GV-SC-06</strong>: 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.</td>
</tr>
<tr>
<td><strong>DATA-P8</strong>: Business Environment: 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).</td>
<td><strong>GV-AM-04</strong>: Potential impacts and likelihoods of threats exploiting vulnerabilities are identified and recorded.</td>
<td><strong>GV-AM-05</strong>: Threats, vulnerabilities, likelihoods, and impacts are used to determine risk and inform risk prioritization.</td>
</tr>
<tr>
<td><strong>DATA-P9</strong>: The organization's role in the supply chain is identified and communicated.</td>
<td><strong>GV-AM-06</strong>: Risks are determined and communicated.</td>
<td><strong>GV-AM-05</strong>: Threats, vulnerabilities, likelihoods, and impacts are used to determine risk and inform risk prioritization.</td>
</tr>
<tr>
<td><strong>DATA-P10</strong>: Priority for organizational mission, objectives, and activities is established and communicated.</td>
<td><strong>GV-DE-01</strong>: The organizational mission is understood and informs cybersecurity risk management.</td>
<td><strong>GV-OC-06</strong>: Outcomes, capabilities, and services that the organization depends on are determined and communicated.</td>
</tr>
<tr>
<td><strong>DATA-P11</strong>: Organizational communication and data flows are mapped.</td>
<td><strong>GV-DE-06</strong>: Outcomes, capabilities, and services that the organization depends on are determined and communicated.</td>
<td><strong>GV-OC-05</strong>: Outcome, capabilities, and services that the organization depends on are determined and communicated.</td>
</tr>
<tr>
<td><strong>DATA-P12</strong>: Systems/products/services that support organizational priorities are identified and key requirements communicated.</td>
<td><strong>GV-DE-02</strong>: Outcome, capabilities, and services that the organization depends on are determined and communicated.</td>
<td><strong>GV-OC-06</strong>: Outcomes, capabilities, and services that the organization depends on are determined and communicated.</td>
</tr>
<tr>
<td><strong>DATA-P13</strong>: Systems/products/services that support organizational priorities are identified and key requirements communicated.</td>
<td><strong>GV-DE-03</strong>: Outcome, capabilities, and services that the organization depends on are determined and communicated.</td>
<td><strong>GV-OC-06</strong>: Outcomes, capabilities, and services that the organization depends on are determined and communicated.</td>
</tr>
<tr>
<td><strong>DATA-P14</strong>: Risk responses are identified, prioritized, and implemented.</td>
<td><strong>GV-DE-04</strong>: Risk impacts and likelihoods of threats exploiting vulnerabilities are identified and recorded.</td>
<td><strong>GV-AM-06</strong>: Risk impacts and likelihoods of threats exploiting vulnerabilities are identified and recorded.</td>
</tr>
<tr>
<td><strong>DATA-P15</strong>: Risk responses are identified, prioritized, and implemented.</td>
<td><strong>GV-DE-05</strong>: Risk responses are identified and prioritized.</td>
<td><strong>GV-AM-05</strong>: Threats, vulnerabilities, likelihoods, and impacts are used to determine risk and inform risk prioritization.</td>
</tr>
<tr>
<td><strong>DATA-P16</strong>: Potential business impacts and likelihoods are identified.</td>
<td><strong>GV-DE-06</strong>: Risk impacts and likelihoods of threats exploiting vulnerabilities are identified and recorded.</td>
<td><strong>GV-AM-06</strong>: Risk impacts and likelihoods of threats exploiting vulnerabilities are identified and recorded.</td>
</tr>
<tr>
<td><strong>DATA-P17</strong>: Threats, vulnerabilities, likelihoods, and impacts are used to determine risk.</td>
<td><strong>GV-DE-07</strong>: Outcomes, capabilities, and services that the organization depends on are determined and communicated.</td>
<td><strong>GV-AM-05</strong>: Threats, vulnerabilities, likelihoods, and impacts are used to determine risk and inform risk prioritization.</td>
</tr>
<tr>
<td><strong>DATA-P18</strong>: Cybersecurity strategy, and priorities and are communicated and enforced.</td>
<td><strong>GV-DE-05</strong>: Risk responses are determined and communicated.</td>
<td><strong>GV-AM-05</strong>: Threats, vulnerabilities, likelihoods, and impacts are used to determine risk and inform risk prioritization.</td>
</tr>
<tr>
<td><strong>DATA-P19</strong>: Cybersecurity strategy, and priorities and are communicated and enforced.</td>
<td><strong>GV-DE-06</strong>: Risk impacts and likelihoods of threats exploiting vulnerabilities are identified and recorded.</td>
<td><strong>GV-AM-06</strong>: Risk impacts and likelihoods of threats exploiting vulnerabilities are identified and recorded.</td>
</tr>
<tr>
<td><strong>DATA-P20</strong>: Cybersecurity strategy, and priorities and are communicated and enforced.</td>
<td><strong>GV-DE-07</strong>: 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.</td>
<td><strong>GV-AM-05</strong>: Threats, vulnerabilities, likelihoods, and impacts are used to determine risk and inform risk prioritization.</td>
</tr>
<tr>
<td><strong>DATA-P21</strong>: Cybersecurity strategy, and priorities and are communicated and enforced.</td>
<td><strong>GV-DE-05</strong>: Risk responses are determined and communicated.</td>
<td><strong>GV-AM-05</strong>: Threats, vulnerabilities, likelihoods, and impacts are used to determine risk and inform risk prioritization.</td>
</tr>
</tbody>
</table>
Privacy and security policies are established, managed, and agreed to by organizational stakeholders.

Risk Management Strategy (GV.RM-P):
Risk appetite and risk tolerance statements are determined, communicated, and maintained.

Awareness and Training (GV.MT-P):
Users are provided awareness and training so they possess the knowledge and skills to perform general tasks with security risks in mind.

Data Processing Policies, Procedures, and Techniques (PR.PT-P):
Data are destroyed according to policy.

Monitoring and Review (GV.MT-P):
Policies, processes, and procedures for managing cyber risks are reviewed, updated, communicated, and maintained.

Privacy Values, Policies, and Training (GV.AT-P):
Senior executives understand their roles and responsibilities.

Data Processing Management (PR.PS-P):
Data is destroyed according to policy.

Data Processing Polices, Procedures, and Techniques (CT.PO-P):
Policies, procedures, and techniques for managing data processing are established and in place.

Risk Management Strategy (GV.RM-P):
Risk appetite and risk tolerance statements are determined, communicated, and maintained.

Monitoring and Review (GV.MT-P):
Policies, processes, and procedures for managing cyber risks are reviewed, updated, communicated, and maintained.

Privacy Values, Policies, and Training (GV.AT-P):
Senior executives understand their roles and responsibilities.

Data Processing Policies, Procedures, and Techniques (PR.PT-P):
Data are destroyed according to policy.

Monitoring and Review (GV.MT-P):
Policies, processes, and procedures for managing cyber risks are reviewed, updated, communicated, and maintained.

Privacy Values, Policies, and Training (GV.AT-P):
Senior executives understand their roles and responsibilities.

Data Processing Management (PR.PS-P):
Data is destroyed according to policy.
Communicate FIPS (PR-P): Develop and implement appropriate data protection safeguards.

PR.IP-7: System or device configurations permit selective collection or disclosure of data elements.

PR.IP-9: Attribute references are substituted for attribute values.

PR.AA-03: Transparency policies, procedures, and processes for communicating data processing purposes, practices, and associated privacy risks are established and in place.

PR.DS-02: Rules 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-P6: 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-P4: Mechanisms for obtaining feedback from individuals (e.g., surveys or focus groups) about data processing 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.PO-P2: Roles and responsibilities (e.g., public relations) for communicating data processing purposes, practices, and associated privacy risks are established.

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-P6: Records of data disclosures and sharing are maintained and can be accessed for review or transmission/disclosure.

CM.PO-P5: Data corrections or deletions can be communicated to individuals or organizations (e.g., data sources) in the data processing ecosystem.

CM.PO-P4: Data protection and usage measures are maintained and can be accessed for review or transmission/disclosure.

CM.PO-P3: Data privacy awareness training is maintained and used to manage the protection of data.

CM.PO-P2: System/product/service design enables data processing viability.

CM.PO-P1: Transparency policies, processes, and procedures for communicating data processing purposes, practices, and associated privacy risks are established.

Data Protection Practices, 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-P9: Identify and define incident response and recovery plans (Incident Response and Recovery) and business continuity plans (Business Continuity) and recovery plans (Incident Response and Recovery) are developed, owned, and tested.

PR.PO-P8: Business continuity and recovery plans are developed, owned, and tested.

PR.PO-P7: Business continuity and recovery plans are developed and implemented.

PR.PO-P6: Business continuity and recovery plans are developed and implemented.

PR.PO-P5: Policies and procedures regarding the physical operating environment for organizational assets are maintained, and tested.

PR.PO-P4: Policies and regulatory influences regarding the physical operating environment for organizational assets are maintained, and tested.

PR.PO-P3: Policies and procedures are established and maintained.

PR.PO-P2: Policies and procedures are established and maintained.

PR.PO-P1: Policies and procedures are established.

PR.IP-P2: The policy and operational strategy (e.g., operation of personnel screening) for identifying, preventing, and mitigating risks to personal privacy and organizational assets are maintained, and tested.

PR.IP-P1: The policy and operational strategy (e.g., operation of personnel screening) for identifying, preventing, and mitigating risks to personal privacy and organizational assets are established and in place.

PR.IP-P0: The policy and operational strategy (e.g., operation of personnel screening) for identifying, preventing, and mitigating risks to personal privacy and organizational assets are established.

Identity, 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-7: Identities are proofed and bound to credentials based on the context of interactions.

PR.AC-6: Identities are proofed and bound to credentials based on the context of interactions.

PR.AC-5: Identities are proofed and bound to credentials based on the context of interactions.

PR.AC-4: Identities are proofed and bound to credentials based on the context of interactions.

PR.AC-3: Identities are proofed and bound to credentials based on the context of interactions.

PR.AC-2: Identities are proofed and bound to credentials based on the context of interactions.

PR.AC-1: Identities are proofed and bound to credentials based on the context of interactions.

PR.AC-P6: Identities and credentials are issued, managed, verified, revoked, and audited for authorized individuals, processes, and devices.

PR.AC-P5: Identities and credentials are issued, managed, verified, revoked, and audited for authorized individuals, processes, and devices.

PR.AC-P4: Identities and credentials are issued, managed, verified, revoked, and audited for authorized individuals, processes, and devices.

PR.AC-P3: Identities and credentials are issued, managed, verified, revoked, and audited for authorized individuals, processes, and devices.

PR.AC-P2: Identities and credentials are issued, managed, verified, revoked, and audited for authorized individuals, processes, and devices.

PR.AC-P1: Identities and credentials are issued, managed, verified, revoked, and audited for authorized individuals, processes, and devices.

PR.AC-P0: Identities and credentials are issued, managed, verified, revoked, and audited for authorized individuals, processes, and devices.

PR.AI-02: Software is maintained, replaced, and removed to eliminate vulnerabilities in assets.

PR.AI-01: Vulnerabilities in assets are identified, validated, and recorded.

PR.AI-00: Vulnerabilities in assets are identified, validated, and recorded.

PR.PS-01: Configuration management practices are applied.

PR.PO-04: The organization's technology assets are protected from environmental threats.

PR.PO-03: The organization's technology assets are protected from environmental threats.

PR.PO-02: The organization's technology assets are protected from environmental threats.

PR.PO-01: The organization's technology assets are protected from environmental threats.

PR.PO-P3: Systems, hardware, software, and services are managed throughout their life cycle.

PR.PO-P2: Systems, hardware, software, and services are managed throughout their life cycle.

PR.PO-P1: Systems, hardware, software, and services are managed throughout their life cycle.

PR.PO-P0: Systems, hardware, software, and services are managed throughout their life cycle.

PR.IP-P9: Systems, hardware, software, and services are managed throughout their life cycle.

PR.IP-P8: Systems, hardware, software, and services are managed throughout their life cycle.

PR.IP-P7: Systems, hardware, software, and services are managed throughout their life cycle.

PR.IP-P6: Systems, hardware, software, and services are managed throughout their life cycle.

PR.IP-P5: Systems, hardware, software, and services are managed throughout their life cycle.

PR.IP-P4: Systems, hardware, software, and services are managed throughout their life cycle.

PR.IP-P3: Systems, hardware, software, and services are managed throughout their life cycle.

PR.IP-P2: Systems, hardware, software, and services are managed throughout their life cycle.

PR.IP-P1: Systems, hardware, software, and services are managed throughout their life cycle.

PR.IP-P0: Systems, hardware, software, and services are managed throughout their life cycle.

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-P5: Systems/products/services and associated data are formally managed throughout removal, transfer, and disposition.

PR.DS-P4: Systems/products/services and associated data are formally managed throughout removal, transfer, and disposition.

PR.DS-P3: Systems/products/services and associated data are formally managed throughout removal, transfer, and disposition.

PR.DS-P2: Data in-transit is protected.

PR.DS-P1: Data at-rest is protected.

PR.DS-P0: Data at-rest is protected.

PR.PO-05: The confidentiality, integrity, and availability of data are protected.

PR.PO-04: The confidentiality, integrity, and availability of data are protected.

PR.PO-03: The confidentiality, integrity, and availability of data are protected.

PR.PO-02: The confidentiality, integrity, and availability of data are protected.

PR.PO-01: The confidentiality, integrity, and availability of data are protected.

PR.PO-00: The confidentiality, integrity, and availability of data are protected.
<table>
<thead>
<tr>
<th>PR.DS-P4:</th>
<th>Adequate capacity to ensure availability is maintained.</th>
</tr>
</thead>
<tbody>
<tr>
<td>PR.DS-P5:</td>
<td>Protections against data leaks are implemented.</td>
</tr>
<tr>
<td>PR.DS-P6:</td>
<td>Integrity checking mechanisms are used to verify software, firmware, and information integrity.</td>
</tr>
<tr>
<td>PR.DS-P7:</td>
<td>The development and testing environment(s) are separate from the production environment.</td>
</tr>
<tr>
<td>PR.DS-P8:</td>
<td>Integrity checking mechanisms are used to verify hardware integrity.</td>
</tr>
<tr>
<td>PR.DS-P9:</td>
<td>Integrity checking mechanisms are used to verify software, firmware, and information integrity.</td>
</tr>
<tr>
<td>PR.MA-P1:</td>
<td>Maintenance and repair of organizational assets are performed and logged, with approved and controlled tools.</td>
</tr>
<tr>
<td>PR.MA-P2:</td>
<td>Remote maintenance of organizational assets is approved, logged, and performed in a manner that prevents unauthorized access.</td>
</tr>
<tr>
<td>PR.PT-P1:</td>
<td>Removable media is protected and its use restricted according to policy.</td>
</tr>
<tr>
<td>PR.PT-P2:</td>
<td>Communications and control networks are protected.</td>
</tr>
<tr>
<td>PR.PT-P3:</td>
<td>Mechanisms (e.g., failover, load balancing, hot swap) are implemented to achieve resilience requirements in normal and adverse situations.</td>
</tr>
</tbody>
</table>

**Maintenance (PR.MA-P):** System maintenance and repairs are performed consistent with policies, procedures, and agreements.

**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, procedures, and agreements.