#	Organization	Commentor	Type	Page #	Line #	Section	Comment (Include rationale for comment)	Suggested change
1	Microsoft	S. Branam	E	13	466 - Framework Core Table	Appendix A	Modify "Asset Management" by adding "Data". Further, a definition of Data should be added to the Glossary and make clear PII is a data element to be protected like any other data element that may be implicated in cybersecurity attacks. As part of these recommended edits, we have focused on consistency in terminology throughout the Framework. Throughout, the terms “data” and “assets” are used interchangeably (as well as "resources" and "information" in certain instances). However, “data” and “assets” carry different meanings in the industry. Generally, assets are tangible and intangible things that have value, and in the cybersecurity context, those things of value are the systems, networks, devices and data. Thus, “assets” are the broad category, of which “data” is a component, and more specifically, PII is a component of “data”. As such, there should be careful application of specific measures to assets versus data, as the requirements are not interchangeable in all instances.	"The personnel, devices, systems, Data, and facilities that enable the organization to achieve business purposes…"
2	Microsoft	S. Branam	E	13	ID.AM-3	Appendix A	Per suggested defined term and ensure consistency.	Capitalize "Data".
3	Microsoft	S. Branam	E	14	ID.AM-5	Appendix A	Per suggested defined term and ensure consistency.	Capitalize "Data".
4	Microsoft	S. Branam	E	14	ID.AM-6	Appendix A	Roles and responsibilities should be established for both cybersecurity and privacy in coordination with one another. May be duplicative of ID.GV-2. Example of PbD.	Add "and privacy" after "cybersecurity".
5	Microsoft	S. Branam	E	14	BE	Appendix A	Roles and responsibilities should be established for both cybersecurity and privacy in coordination with one another. May be duplicative of ID.GV-2. Example of PbD.	Add "and privacy" after "cybersecurity".
6	Microsoft	S. Branam	E	15	ID.GV-1	Appendix A	Policies related to cybersecurity and privacy should be established in coordination with one another. Example of PbD.	Add "and privacy" after "security".

7	Microsoft	S. Branam	E	15	ID.GV-2	Appendix A	Roles and responsibilities should be established for both cybersecurity and privacy in coordination with one another. May be duplicative of ID.AM-6. Example of PbD.	Add "and privacy" after "security".
8	Microsoft	S. Branam	E	15	ID.GV-4	Appendix A	A governance program should consider the privacy implications of the program.	Add "and consider the privacy implications of its cybersecurity program" after "cybersecurity risks".
9	Microsoft	S. Branam	E	15	RA	Appendix A	Per suggested defined term and ensure consistency.	Capitalize "Assets" in Category statement of RA.
10	Microsoft	S. Branam	E	16	ID.RA-3	Appendix A	Per suggested defined term and ensure consistency.	Capitalize "Assets".
11	Microsoft	S. Branam	E	16	AC	Appendix A	Per suggested defined term. The Framework uses "resources", "assets", "information" and "records" interchangeably which causes confusion and ambiguity. Best to use defined terms and be consistent.	Replace "information resources and associated facilities are" with "organizational Assets is".
12	Microsoft	S. Branam	E	17	PR.AC-2	Appendix A	Per suggested defined term and ensure consistency.	Replace "resources" with "Assets".
13	Microsoft	S. Branam	E	17	AT	Appendix A	Important to ensure both cybersecurity and privacy training and awareness occurs. Example of PbD.	Insert "and privacy" after "information security".
14	Microsoft	S. Branam	E	18	DS	Appendix A	Per suggested defined term and ensure consistency. "Information and records (data)" is confusing and inconsistent. The scope of the Data Security category is in relation to "Data", and the text should reflect such.	Replace "Information and records (data) are" with "Data is". Remove "information" after "availability of" and replace with "Data".
15	Microsoft	S. Branam	E	18	PR.DS-3	Appendix A	Per suggested defined term and ensure consistency.	Replace "Assets are" with "Data is".
16	Microsoft	S. Branam	E	19	PR.DS-5	Appendix A	Per suggested defined term and ensure consistency.	Capitalize "Data".
17	Microsoft	S. Branam	E	19	PR.DS-6	Appendix A	Intellectual property is a component of "Data" and is therefore implicitly covered by PR.DS-1 and PR.DS-2.	Remove entirely.
18	Microsoft	S. Branam	E	19	PR.DS-7	Appendix A	Per suggested defined term and ensure consistency. May be duplicative of PR.IP-6.	Replace "assets are" with "Data is".
19	Microsoft	S. Branam	E	19	PR.DS-9	Appendix A	Suggested definition of Data includes PII, therefore is already covered by PR.DS-1 and PR.DS-2. It is confusing to have a specific cite to PII here but not elsewhere.	Delete entirely.
20	Microsoft	S. Branam	E	19	IP	Appendix A	Suggested definition of Assets is inclusive of all corporate systems.	Replace "information systems and assets" with "Assets and considers the privacy implications thereof".
21	Microsoft	S. Branam	E	20	PR.IP-4	Appendix A	Per suggested defined term; scope of this requirement is to ensure all Data is backed up.	Replace "information are" with "Data is".
22	Microsoft	S. Branam	E	20	PR.IP-5	Appendix A	Per suggested defined term and ensure consistency.	Capitalize "Assets".

23	Microsoft	S. Branam	E	20	PR.IP-6	Appendix A	Per suggested defined term and ensure consistency. May be duplicative of PR.DS-7.	Replace "Information" with "Data".
24	Microsoft	S. Branam	E	20	PR.IP-8	Appendix A	Per suggested defined term and ensure consistency.	Replace "Information" with "Data".
25	Microsoft	S. Branam	E	21	PR.IP-11	Appendix A	HR practices should be inclusive of both cybersecurity and privacy. Example of PbD.	Add "privacy" after "Cybersecurity".
26	Microsoft	A. Kleiner	E	21	N/A	Appendix A	Recommend addition of a category and a subcategory focused on secure software development practices. For additional rationale, see Microsoft's comments on the Preliminary Framework.	Add a category, "Secure Engineering (SE): Design and develop technology (e.g., hardware, software and services) in a manner consistent with international standards and industry best practices throughout the engineering lifecycle"; followed by a subcategory, "PR.SE-1: Utilize a recognized secure development lifecycle process that includes guidance on relevant security and privacy practices, controls, and tooling across all phases of the engineering lifecycle (design, develop, review, test, approve)"
27	Microsoft	S. Branam	E	21	MA	Appendix A	Per suggested defined term and ensure consistency.	Replace "operational and information system components" with "Assets".
28	Microsoft	S. Branam	E	21	PR.MA-1	Appendix A	Per defined term and ensure consistency.	Capitalize "Assets".
29	Microsoft	S. Branam	E	21	PR.MA-2	Appendix A	Per suggested defined term and ensure consistency.	Capitalize "Assets" in "organizational assets" and replace "information systems" with "Assets".
30	Microsoft	S. Branam	E	21	PT	Appendix A	Per suggested defined term and ensure consistency. Protective technology may have privacy implications and should therefore be appropriately addressed.	Replace "systems and assets" with "Assets while considering related privacy implications".
31	Microsoft	S. Branam	E	21	PR.PT-1	Appendix A	The audit function implicates privacy and therefore should be addressed specifically in the Framework.	Replace "audit policy" with "audit and privacy policies."
32	Microsoft	S. Branam	E	21	PR.PT-3	Appendix A	Per suggested defined term and ensure consistency.	Replace "systems and assets" with "Assets".
33	Microsoft	S. Branam	E	22	CM	Appendix A	Per suggested defined term and ensure consistency.	Replace "The information system and assets" with "Assets".
34	Microsoft	S. Branam	E	24	RS.CO-2	Appendix A	It is important that event reporting occur in a manner consistent with the organization's cybersecurity and privacy policies. Example of PbD.	Add "and policies related to cybersecurity and privacy" following "established criteria".

35	Microsoft	S. Branam	E	25	RP	Appendix A	Per suggested defined term and ensure consistency.	Replace "systems or assets" with "Assets".
36	Microsoft	A. Kleiner	E	39	645	Appendix C	Add discussion of the emerging practice and standards related to software ID tagging, or SWID. For additional rationale, see Microsoft's comments on the Preliminary Framework.	For example, software ID tagging, or SWID, is an emerging practice related to supply chain risk management. There is a relatively new standard, ISO/IEC 19770-2, that enables developers and users to verify the origin of software. If a user organization understands which suppliers are implementing secure development practices in conformance with ISO 27034-1, application of ISO/IEC 19770-2 enables that organization to confirm that it is using software that came from those suppliers. Currently, NIST's National Cybersecurity Center of Excellence (NCCoE) and DHS are leading efforts to define the government's expectations regarding SWID. Accordingly, as these workstreams continue to development, they will be ripe for consideration and inclusion in future iterations of the Framework.

37	Microsoft	A. Kleiner	E	42	before 688	Appendix E	Recommend addition of a definition for adoption. For additional rationale, see Microsoft's comments on the Preliminary Framework.	**Adoption:** An organization (e.g., critical infrastructure owner or operator) utilizes the Framework as baseline guidance in its determination of appropriate cybersecurity risk management activities and related privacy protection efforts. This process should involve adaptation of the Framework to suit organizational needs, including identification of organization-specific activities that give effect to the goals of the Framework but may not be listed in the Framework. Where an organization has aligned its policies, practices, and procedures with an Informative Reference, or provided self-attestation or certification against an Informative Reference, the organization is operating at a fundamentally mature level of implementation.
38	Microsoft	S. Branam	E	42	before 688	Appendix E	Suggested definition - Asset: The personnel, devices, systems, Data, and facilities that enable the organization to achieve business purposes.	Add a definition of "Asset".
39	Microsoft	S. Branam	E	42	between 696-697	Appendix E	Adding a definition of "Data" would help clarify the scope of application of the various activities in the Framework. The definition should clearly limit the scope to Data implicated by cybersecurity attacks. The definition should make clear that PII is a subcategory of Data.	Add a definition of "Data".
40	Microsoft	S. Branam	E	42	721-725	Appendix E	The definition of PII should be removed. Each sector will define PII differently and therefore, it would be futile for the Framework to attempt a definition that is appropriate for all sectors.	Remove definition of PII.