#	Organization	Commenter	Type	Page #	Line #	Section	Comment (Include rationale for comment)	Suggested change
1				18		Appendix A	PR.AT-3 references the roles and responsibilities of 3rd parties, but there is no process for tracking of such 3rd parties in the Framework. This should be considered as well as identification as an asset type in Asset Management.	
2				25		Appendix A	Consider a sub-category for communications with executive management or BOD during recovery. This is a critical step that is different than public relations or reputation repair.	Suggest adding a RC.CO-3 as a new communications sub-category: "RC.CO-3: Internal stakeholder and executive management communications."
3				25		Appendix A	When sub-categories have the same heading, perhaps they should be combined or better differentiated. RS.IM and RC.IM are related to improvements, and RS.CO and RC.CO are related to communications. They are specific to the Recovery and Response functions which could be combined as one joint category as they share many of the same Informative Reference sections across other frameworks.	
4				28		Appendix B	The privacy discussion is based on a single standard (FIPP) rather than following the approach used in the overall framework of referencing all applicable standards. There are several comprehensive and effective Privacy Frameworks, such as the AICPA, which are better geared towards international privacy requirements.	Use a format similar to the CSF section, with core privacy principles as the functions and the privacy frameworks as references.

5				28		Appendix B	Move existing Governance.ii - v. to Business Environment. Typically, it is the business decision (and their operations) that drive the need for PII to be used, therefore, BE should be the section where the need for PII is captured and documented. Governance should only establish the oversight and review function (e.g., policies, etc.)	
6				31		Appendix B	Security Continuous Monitoring should be worded to include review for compliance with local regulations related to workforce monitoring. There are specific laws (at least in other countries) that limit what can be recorded, viewed, or tracked regarding employee actions and emails. It's hard to ignore international considerations since most companies are now global and have employees / contractors in other countries.	
7							"Cloud" is only mentioned a few times. While these controls can be applied to external service providers and the cloud, perhaps more definition or guidance is warranted. Mention of the CSA frameworks or NIST guidance should be included and perhaps mapped back to the controls, with specific recommendation on which elements apply to cloud environments.	