#	Organization	Commenter	Type	Page #	Line #	Section	Comment (Include rationale for comment)	Suggested change
1	Symantec		G	2	100-104	1	The preliminary Framework rightly recognizes that many organizations that consider adopting it will have existing cybersecurity programs and risk management processes in place. However, the Framework never answers the question of why an organization that has such a program or process should look to the Framework.	Include a statement explaining why an organization that has an existing cybersecurity program should use the Framework.
2	Symantec		G	2	140-142	1.1	Many organizations that adopt the Framework have numerous components within them, and very often each will have a different security requirements and threat profile.	State/recognize that different components of an organization may have different profiles and might implement the framework differently.
3	Symantec		G	6	235-237	2.1	NIST should strengthen and expand its recognition that the Informative References in the Framework are not exhaustive.	Expand the statement to encourage organizations to use any standard - including ones that are internally developed - that achieve a desired security end in the most cost-effective and technologically efficient method possible.
4	Symantec		E	8	308	2.3	The NIST example of a notional flow of information describes "a" notional flow, not "the" notional flow.	Replace "the" with "a."

5	Symantec		G	9	322-331	2.4	NIST representatives stated at the workshops that few organizations will need to strive for “Tier 4: Adaptive” in many of the core functions, and in fact few if any will need to be Tier 4 in all of the functions. NIST acknowledged that reaching and maintaining Tier 4 would be costly (particularly for small and medium businesses) and will often make no sense given a company’s threat profile. The preliminary Framework itself does not reflect this, however.	State clearly and prominently that in most use cases, lower tiers are not only acceptable, but are in fact appropriate. It is important that the Framework not be misinterpreted as a call for all organizations to seek the highest level of security, irrespective of need or cost.
6	Symantec		G	11	399	3.1	The sentence states what cybersecurity measures organizations "should have" in place at the outset. That seems incongruous for a Framework designed to help organizations build capability, including some that are starting from scratch.	Strike clause.
7	Symantec		G	11, 12	417-421	3.2	The "risk assessment" should include valuing what needs to be protected and the potential loss in case of an event.	Edit paragraph accordingly.
8	Symantec		T	14		ID.BE-3	Priorities that are established need to be communicated.	add to line: "and communicated"
9	Symantec		T	19		PR.DS-6	The Subcategory needs to be broader, as organizations needs to protect more than just intellectual property.	Make it more inclusive; suggested language: "Proprietary or non-public business data, intellectual property, and other confidential information is protected"
10	Symantec		T	19		PR.IP-1	Baselines need to be maintained once they are established.	Add "and maintained" at the end.
11	Symantec		E	21		PR-PT-2	Readability - current formulation is awkward.	Change to: "Use of removable media are regulated according to a specified policy"

12	Symantec		T	21, 22		PT; DE.CM-4	Malicious code detection is referenced only under the "DETECT" function. It should be part of the "PROTECT" function as well, so malicious code can be detected *before* it is on a system.	Add a new subcategory under "Protective Technology" for detection of malicious code.
13	Symantec		E	39	639	C.8	Readability	Replace "there remain challenges" with "challenges remain"