#	Organization	Commentor	Type	Page #	Line #	Section	Comment (Include rationale for comment)	Suggested change
1	Leidos	R. Grant	E	i	29	Notes	"specificity" is too vague.	Clarify context of specificity as done in lines 19, 20.
2	Leidos	R. Grant	G	Multiple	Multiple	All	Point to References, as in (See Reference XX). Include an Appendix for References.	Drop the use of Footnotes.
3	Leidos	K. Tydings	G	1	74	1.0	Need stronger message to regulatory entities. The intent would be so they can ensure the organization which they regulate adapt the new framework	Due to the increasing pressures from external threats, regulator entities and organizations responsible for securing the critical infrastructure must have consistent and iterative approach to identifying, assessing, and managing cybersecurity risk.
4	Leidos	R. Grant	E	1	82	1.0	Drop this sentence.	This sentence adds nothing. It restates the obvious.
5	Leidos	R.Grant	E	1	93	1.0	This sentence adds nothing. It restates the obvious.	Drop the sentence that begins, "Market competition…."
6	Leidos	K. Tydings	G	2	103	1.0	Cybersecurity implementation should be defined in part as a means to develop an understanding of the gaps or inadequacies of current, in-place programs and processes and	…organization's management of cybersecurity risk. Cybersecurity implementation is defined in part as a means to develop an understanding of the gaps or inadequacies of current, in-place programs and

#	Organization	Commentor	Type	Page #	Line #	Section	Comment (Include rationale for comment)	Suggested change
							compensating for the gaps or inadequacies.	processes and compensating for the gaps or inadequacies. Alternatively, an organization without an existing cybersecurity program can...
7	Leidos	C. Vee	E	2	103	1.0	Use of the framework can also support common communication of cybersecurity risks.	Recommend adding communication benefit This is raised a bit in 1.2, but believe this also belongs in 1.0
8	Leidos	R. Grant	E	2	106	1.1	The logic is backwards as written. The Framework should be a guide for organizations to align their practices not the other way around.	"….to align this guidance…." should be changed to "….to align their risk practices with the guidance."
9	Leidos	R. Grant	E	2	112	1.1		Replace "detailed" with "explained."
10	Leidos	R. Grant	E	2	125-130		These lines go into too much detail for an Overview	Drop these lines. Possibly move them to another section.
11	Leidos	R.Grant	G	2	131	1.1	The "Appendix B" is reference out of place, an afterthought.	This discussion of privacy and civil liberties might fit better at the end of the Section.
12	Leidos	A.K. Aslam	G	2	141, 142	1.1 Overview of the Framework	Framework Categories and Subcategories are introduced without properly defining what those terms.	Include definitions of the new terms
13	Leidos	R. Grant		3	144	1.1	Change "are" to "can."	"Can" sounds better in this sentence.

#	Organization	Commentor	Type	Page #	Line #	Section	Comment (Include rationale for comment)	Suggested change
14	Leidos	R. Grant	E	3	170	1.2	Change "inform" to "identify."	"Inform" is used throughout the document. It seems weak. It should be changed to more decisive verbs wherever possible.
15	Leidos	K. Tydings	G	3	183	1.2	Having an awareness that risk to an organization responsible for securing the critical infrastructure exists to capture the attention of both an assessor and an organization within the critical infrastructure should be developed. Due to a passive approach so far in some industries, I believe this message should be clear.	...risk-based to provide flexible implementation. Organizations responsible for securing the critical infrastructure should adapt the understanding that (a) there are threats to the various IT and ICS systems within critical infrastructure and (b) the systems within their organizations are at risk to vulnerability exploitation.
16	Leidos	A.K. Aslam	E	4	186, 187	1.3 Document Overview	Maintain the order of framework components.	…Framework Core, the Profile and Tiers
17	Leidos	R. Grant	E	5	201	2	" both internally and externally." don't add anything to the sentence. Externally doesn't make any sense in the context of the Framework.	Drop "internally and externally."

#	Organization	Commentor	Type	Page #	Line #	Section	Comment (Include rationale for comment)	Suggested change
18	Leidos	C. Vee	G	5	208	2.1	While the framework itself is not a checklist it feels like the document is not recognizing the benefit of checklists to enable standard processes and configurations	Recommend adding checklists to line 210 as a potential outcome of the framework
19	Leidos	R. Grant	G	6	243	2.1	**Identify** does not explicitly include threats in this discussion. Line 249 mentions risks.	Include threats in this section.
20	Leidos	R. Grant	E	7	255		The Categories are not outcomes, they are activities.	Change "outcomes:" to "activities:"
21	Leidos	R. Grant	G	7	290	2.1	Are there any Target Profiles that already exist?	Identify a link to examples of Target Profiles.
22	Leidos	R. Grant	E	8	297	2.2		Change "serve" to "serves" and replace "part" with "input."
23	Leidos	R. Grant	E	9	318	2.3	Figure mentions Risk Appetite. This is the only place in the document that this term is used.	Recommend changing "Risk Appetite" to "Risk Tolerance" in Figure to be consistent with the rest of the document.
24	Leidos	A.K. Aslam	T	11	390	3.0 How to Use the Framework	score card and a diagram connecting framework cores, profiles and tiers would help a reader.	Appendix-A_framework-core-informative-references provides tabular reference. However, it would be nice to have a pictorial flowchart as well. score card of how an organization is scoring in each of the areas would be helpful.
25	Leidos	A.K. Aslam	T	13	457	Appendix A: Framework Core	Guidance on 3rd party supplier in not mentioned under any category. Reality of	Include verbiage on supplier security quality assessment and establishment of vendor

#	Organization	Commentor	Type	Page #	Line #	Section	Comment (Include rationale for comment)	Suggested change
							today's businesses is they have many suppliers supporting their mission and the quality of their security controls is as important as their internal controls.	management process.
26	Leidos	A.K. Aslam	G	15		Governance (GV)	Include Standards along with the policies, procedures and processes	Standards like NIST STIGs, CIS guidelines can be good examples
27	Leidos	A.K. Aslam	G	15		Risk Assessment (RA)	The verbiage for RA is more appropriate in Risk Management (RM) section	This section should include risk rating, methodology, and decision capture process.
28	Leidos	A.K. Aslam	G	19		Information Protection Processes and Procedure (IP)	Include Standards along with the policies, procedures and processes	Standards like NIST STIGs, CIS guidelines can be good examples
29	Leidos	A.K. Aslam	G	21		Maintenance (MA)	Maintenance of an information system include proper disposal process	Maintenance, repair, and disposal of ….
30	Leidos	R. Grant	E	26	469	Appendix A	These references hand out like an afterthought.	Ad an additional Appendix of References.
31	Leidos	R. Grant	E	27	478	Appendix A	Lines 478 through 483 seem to be out of place. They don't add any clarity to Table 1.	Drop these lines.
32	Leidos	R. Grant	E	27	484	Appendix A	Table doesn't add anything to the Appendix. Table 1 is sufficiently clear to stand on its own.	Drop Table 2.

#	Organization	Commentor	Type	Page #	Line #	Section	Comment (Include rationale for comment)	Suggested change
33	Leidos	R. Grant	E	36	509, 510	Appendix C	Line 500 identifies the areas for improvement as Initial. This implies that there could be more. Lines 509 and 510 say the same thing.	Drop lines 509 and 510.
34	Leidos	A.K. Aslam	G	36	493	Appendix C	This seems to be standing by its own without any reference in the main box of the document	reference should be made to Appendix in the body of the document or take it out as a supplemental information.
35	Leidos	R. Grant	E			Alternative Appendix A	Appendix is clear and informative. Alternative Appendix does not offer any improvement over it	Keep Appendix A.