#	Organization Name	Submitted By	Type*	Page #^	Starting Line #^	Ending Line #	Section #	Comment (Include rationale for comment)^	Suggested Change^
1	National Defense Industrial Association (NDIA) - Cybersecurity Division	Law & Policy Committee	G	2	224	242	Intro	NIST SP 800-171B states that it will apply to contractors that are involved in High Value Asset (HVA) or Critical Programs . • Can a succinct definition of a HVA be given? • What is a Critical Program?	• A succinct definition of a HVA should be given considering its importance to 800-171B. Footnote 6 references to publications that provide a comprehensive overview of the HVA Program, but it would be helpful to the reader to have a definition in the NIST publication. • Provide a definition for "Critical Program."
2	NDIA	Law & Policy Committee	G	6	335	341	2.2	Insertion of "Discussion sections" expands scope of controls from Appendix into 171A rev2 and 800-171B.	The NIST 800-171 Rev 1 document made clear that the "discussion" section accompanying each control did not change the scope of each control for the purpose of audits or assessments. Specifically, it included this language: "The discussion is not intended to extend the security requirements or the scope of the assessments of those requirements" (emphasis in original). However, the corresponding language in the draft NIST 800-171B and NIST 800-171 Rev 2 documents drops the language regarding scope of assessments and only states, "The discussion section is not intended to extend the scope of the requirements." In addition, the control discussion sections in the draft NIST 800-171 Rev 2 document no longer appear in an appendix and now appear right next to each corresponding control, and the NIST 800-171 B document is similarly structured. These language and structural changes will lead to a new source of confusion about whether the discussion language changes the scope of each underlying control. We recommend 1) inserting clear language in both the draft NIST 800-171B and NIST 800-171 Rev 2 documents making clear that the discussion sections do not expand the scope of each control for the purpose of audits or assessments, and 2) moving the control "discussion" sections in the draft NIST 800-171B and NIST 800-171 Rev 2 to an appendix for each document rather than including them next to each corresponding control.
3	NDIA	Law & Policy Committee	G	29	956	975	3.13.3e	Requirement 3.13.3e provides that companies can implement disinformation 1. How can the NIST require contractors to have a program like this without also including Govt involvement? 2. How can NIST provide for this requirement without acknowledging how cost prohibitive it is? 3. If this disinformation tactic is used, shouldn't it be a qualified requirement that assumes that implementing entities (contractors) have been provided some form of indemnification? (i.e. Government contractor defense; PL 85-804 (indeminification).	The disinformation tactic should not be required unless the open questions are addressed.