Organization Name^	Submitted By^	Type*	Page #^	Starting Line #^	Ending Line #	Section #	Comment (Include rationale for comment)^	Suggested Change^
Boeing	R.A. Renk		1	191	191		Note 4 has the incorrect EO reference. It reads EO 13526. I bleive what is intended is 13556	Change EO reference to EO 13556
Boeing	R.A. Renk		7	362	262	3.8	Just FYI: The DoD does NOT recognize this marking direction. They continue to publish a policy that says CUI will be marked and handled in accordance with DoDI 5200.01 Vol 4.	Suggest putting in a note that recogonizes this discrepancy. In spite of 32 CFR 2002 requiring NIST 800-171 apply to all CUI in all executive agencies, the DoD is the only known agency even requiring NIST 800-171. Even NASA's policy retains their "Sensitive by Unclassified" policy.
Boeing	R.A. Renk		9	428	431		Adding this sentence about using SSPs for risk management decision does not contribute to the NIST mission of establishing cybersecurity control requirements. It ventures into the arena of procurement policy and has some competition issues that NIST might not want to be involved with.	Recommend deleting this sentence. (and lines 1530 through 1533)
Boeing	R.A. Renk		20	806	807		This requirement discusses identifying individual users. However, the discussion in lines 1026 through 1028 suggests this is not applicable for "group accounts". Also, lines 798 through 799 again recognize the existance of group accounts. There is some confusion between whether complicance to 3.3.2 can be achieved if "group accounts" are used. This is particular acute when fielded weapons system are developed and deployed in a manner that are required to NOT required individual weapons users to logon individually. The defense contractor then must have development tools that mimic the deployed configuration and thus can't have individual logon functionality	Perhaps some additional discussion or explanation would be appropriate to recognize this dilema and provide so requirement "relief". For example, something like "...when groups accounts are operationally required, individual identification of user activity is not require." Or perhaps in 3.3.2 the words could be: " Except for operationally required group accounts, ensure that the actions of individuals...."

^ Required Field
*Type: E - Editorial, G - General T - Technical

Organization Name^	Submitted By^	Type*	Page #^	Starting Line #^	Ending Line #	Section #	Comment (Include rationale for comment)^	Suggested Change^
Boeing	R.A. Renk		20	813	814		Not sure how temperature and humidity contribute to indentication of individual system users.	Perhaps investigate whether temp and humidity really are probative factors for individual user identification and adjust the sentence as appropriate
Boeing	R.A. Renk		27	1055	1055		Note 24: Consider a "location based" factor as an addition method. For example, if the information system is physically protected for access control purposes. Hence, for an unauthorized "user" should not even have physical access. That is a very positive deterrent for unauthorized access.	
Boeing	R.A. Renk		34	1237	1247		Consider addressing the photographic images issues associated the printed and digitally stored photo images. This also means that a "camera" becomes an information system when CUI is involved.	The overal focus of cybersecurity tends to be based on computer securiyt and network security. The traditional physical security issues tend to be over-shadowed by the cyber-oriented SMEs. That is, section 3.8, 3.9 and 3.10 tend to be addresses by "the other guys". And the "the guys" (traditional industrial security people) have been "traditionally" not concerned with "unclassified information". Providing examples of the cross-over of CUI into the traditional ways might aid in the cultural adjustments of controlling unclassified data is a digitally dominated age.