#	Organization Name^	Submitted By^	Type*	Page #^	Starting Line #^	Ending Line #	Section #	Comment (Include rationale for comment)^	Suggested Change^
	Boeing	R.A. Renk		ii	70	70	Keywords	DFARS 252.204-7012 make a clear distinction of "Covered Contract Information Systems" when they impose NIST (SP) 800-171. It would be advantageous to use the same term versus "contractor system". If that is not possible, perhaps a definition in the Glossary making a clear distinction between the two terms which have the high probability of being used colloquially as the same thing by the current predominate audience of NIST 800-171 (e.g. the DoD community).	Note: Only the DoD provided any NIST published commentary to how 800-171B would be used.
	Boeing	R.A. Renk		1	205	205		Note 4 has the incorrect EO reference. It reads EO 13526. I believe what is intended is 13556	Change EO reference to EO 13556
	Boeing	R.A. Renk		1	210	210		Recommend new paragraph at end of sentence on this line.	
	Boeing	R.A. Renk		8	367	377		The intent of this section appears unclear about what the criteria is for determining what needs to be protected from APT threats using the enhanced controls. • Line 367/368 clearly indicate it is the confidentiality of CUI. The point here is that it is the information that needs protection from unauthorized disclosure due to APT. This seems to be the appropriate fundamental principle. • Line 370 then gives the agency the authority to determine and designate what information needs protection…whether or not it is CUI. Again appropriately fundamental. • But Line 371 introduces the confusion with the addition of two "OR's": …or a system as a critical program…or a high value asset…This redirects to criteria away from the information and to the program or to a high value asset. • Then Note 17 completes the confusion or purposefully declaring that it is no longer the value of the information that could be disclosed to an unauthorized individual but it is the value of the "program" or the "value of the asset" that needs protection. This seems fundamentally in error. If the value of a piece of information on a $10 memory stick is important (e.g. "critical") to an executive agency, it seems it should be protected even if not on a Trinity Supercomputer system.	• Refocus this introduction section to focus on the value of the ***information*** as determined by the agency and employ the enhance control requirements on any information system or component that processes, stores, or transmit that information. Furthermore, clarify that it's not just any information as line 370 suggest but only CUI. (Hence, an agency/program must declare "any information" they want protected via enhance controls IAW NIST 800-171B as CUI appropriately through the CUI Registry. • Additionally, remove the idea that these enhanced controls can only be applied to components that process, store, or transmit such high value CUI. That is, do not prevent as line 375 does from using these controls as desired by any agency or entity to improve their cybersecurity posture for "non-high value CUI" or a "non-critical" program. An overanxious auditor might consider "only" as such enhanced controls should NOT be used on non-critical or non high value assets. (I have seen such interpretations in audit findings).
	Boeing	R.A. Renk		9	411			Observation: Note 21: NIST 800-53 Rev 5 does not exist yet in a released/approved form. It was last publically disclosed in draft almost two years ago.	Perhaps releasing NIST 800-53 Rev 5 is the optimum recommendation. But if it is not yet ready, perhaps acknowledging this unapproved state within the boundaries of this document should it be released before 800-53 is released.
	Boeing	R.A. Renk		12	471	+		Observation: The numbering schema of appending an "e" to the end of the existing control numbers might have an alternative.	Consider a control numbering schema that adds these controls with numbers that flows at the end of the existing basics and derived requirements versus appending an "e" to existing control numbers. This would improve the sorting and traceability of controls to implementation solutions. It will also avoid confusion when trying to verbally discuss control 3.1.1 "or did you mean 3.1.1 "eee"? (Recommended Longer term solution is to combine 800-171B with 800-171 and have Basic, Derived, and Enhanced controls. Then only one document to manage and reduces substantial duplication. The procurement agency can select requirements to impose similar to how is often done with 800-53.)
	Boeing	R.A. Renk		12	471	482	3.1.1	This requirement needs to be bounded in some manner. Using dual authentication on a "critical programs" and "high value assets" for ***all*** its "critical or sensitive systems ***AND*** organization operations might not be a cost effective solution in view of the risks associated with that organization's operations.	Perhaps adjust the requirement to "Document in the SSP the critical or sensitive systems and organizational operations that will employ dual authorization". Then in the discussion area talk about benefits of and criteria for selecting those systems and operations within that organization or program that would benefit from dual authorization.
	Boeing	R.A. Renk		12	483	483	3.1.2	This requirement makes the program or high value asset "compartmentalized". It prevents collaborative efforts between the agency and the contractors supporting that agency. This control needs some flexibility.	For example, change "restrict" to "Control" and change "issued" to "authorized". Leave it to the agency to decide how to control and authorize in their SSP.
	Boeing	R.A. Renk		25	750	768	3.11.2	Making this a control requirement for non-federal organizations may be difficult to comply with since it borders on potentially criminal activity for non-state players. This is particularly acute in the absence of "internal organizational systems" in the universe of systems to hunt.	Recommend deliberately mentioning that the "hunting grounds" are restricted to "systems" under control of the organization.
	Boeing	R.A. Renk		25	769	771	3.11.2	Note: Although offensive cybersecurity (e.g. hunting) activity is a 2018 National cyber policy, none of the references deal with offensive activity.	Recommend putting in a reference or creating such guidance discussing "hunting" techniques available to non-federal entities.
	Boeing	R.A. Renk		25	770	770		NIST 800-160-2 is not a released publication yet. The draft is 18 months old.	Perhaps releasing NIST 800-160-2 is the optimum recommendation. But if it is not yet ready, perhaps acknowledging this unapproved state with the boundaries of this document should it be released before 800-160-2 is released.

^ 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		26	787	789	3.11.4	An SSP documents the "how" and "what" an organization does to accomplish cybersecurity control requirements. To also include the "why" distracts from the objective of telling general users what or how to accomplish something. Additionally, 800-171r2 reference SSP template does not have a "structure" to accommodate a "why" for controls And the "why" is not a NIST 800-171r2 control # 3.12.4 objective.	Consider either requiring a written risk assessment analysis to document the "Why". Alternatively move this requirement to the 3.12.4 section of this document and modify the words to say: Modify the SSP to include a risk assessment section to identify the risk basis for the enhanced controls implemented. But before that, consider whether the existing 800-171r2 control # 3.11.1 already accomplished the intent of periodically re-evaluating the risks and the "why" the organization controls are effective.
	Boeing	R.A. Renk		26	805	806	3.11.5	NIST 800-171r2 control # 3.11.1 already requires an effectivity assessment. If ATP is truly as fast paced as suggested, then an annually assessment will actually be detrimental by providing a false sense of security.	Rather consider implementing a pro-active Threat Assessment Working Group and move this control requirement into the 3.6 area as a compliment to the "reactive" SOC and the "reactive" response team. Make this "assessment" a continuous process to apply lessons learned from incidences and the knowledge gained sharing information via cybersecurity cooperatives
	Boeing	R.A. Renk		29	877	877	3.13.1	This is a "solution" and should not be a requirement. It is mandating an architecture and design solution that might not be cost effective and induce non-capabilities which could hamper the speed at which countermeasures can actually be employed.	Consider placing this solution into the control requirement discussion area for consideration as an architectural solution. (Maybe the discussion section of 3.11.4 might be a place to have an enhanced discussion of the benefits of this solution)
	Boeing	R.A. Renk		33	1045	1045	3.14.2	This requirement appears to duplicate what is already required in NIST 800-171 Rev 2 Control # 3.14.7 and 3.3.5.	If this is not a duplication, perhaps enhancing the discussion with where this requirement picks up after 3.14.7 and 3.3.5 stops would help clarify the intent.
	Boeing	R.A. Renk		34	1068	1068	3.14.3	All of these concepts of an information system are already required for CUI protection in NIST 800-171r2. Note 1 in NIST 800-171r2 and even the definition of an Information system on page vi on NIST 800-171r1 uses these terms directly (or the terms used in definitions of OT and IIOT). Hence, if a program is considered critical or the assets are high value, all of these information system concepts already apply. Therefore, this control requirement is distilled into saying to comply with all of the requirements of NIST 800-171B or isolate the network. This seems redundant and thus worthy of deletion. But I suspect more was intended here. It is just not clear what this control requirement would be that is not already required (except the solution to "isolate" the system).	Delete and make the point more clear in NIST 800-171 Rev 2 if it not already there. Alternatively, if NIST 800-171 Rev 2 does not embrace these concepts of an information system, then enhance the discussion in 800-171B where these concepts of an information system are only part of a "critical program" or "high value asset".
	Boeing	R.A. Renk		35	1137	1138	3.14.5	Consider whether there is an cybersecurity advantage of actually retaining CUI that is no longer needed. For example, usually only the knowledgeable program players know what is needed or not needed. The adversary does not now this. Why do his/her filtering for them? Another example: extracting large files of data makes the adversary's presence more persistent, visible and its easier to identify the suspicious activity. Finally, obfuscation, distraction, and delaying the understanding data are all countermeasures in which retaining unused data can be used for.	Just consider whether this is actually a cybersecurity protective measure or an innate desire to implement data management techniques from a pre-cyber threat world.
	Boeing	R.A. Renk		9	431			Note 22: The link goes to the NARA link at the end of the document not the intended NIST entry.	

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