#	Organization Name^	Submitted By^	Type *	Page #^	Starting Line #^	Ending Line #		Comment (Include rationale for comment)^	Suggested Change^
	General Atomics	Alfred Knoll		ii	61	63	Abstract	The conditions for implementing 800-171B include Item (3), "where there are no specific safeguarding requirements for protecting the confidentiality of CUI prescribed by the authorizing law, regulation, or governmentwide policy for the CUI category listed in the CUI Registry". This condition does not apply since NIST 800-171, R1, exists and it's use is mandated through the CUI Registry under the Controlled Technical Information category under the authority of the DFARS 252.204-7012. Rationale: This condition negates any requirement to employ the 171B controls for any entity that must comply with the DFARS clause.	Delete.
	General Atomics	Alfred Knoll		All	All	All	Entire	The entire document refers to "critical programs and high value assets". However, neither term is defined in the glossary and the process for determining and designating critical programs or high value assets is not included. Rationale: Lack of defined terms and processes create ambiguity leading to inconsistent application of controls.	Include definitions in Glossary and identify the proscriptive process for determining high value assets.

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

#	Organization Name^	Submitted By^	Type *	Page #^	Starting Line #^	Ending Line #		Comment (Include rationale for comment)^	Suggested Change^
	General Atomics	Alfred Knoll	General	All	All	All	Entire	This publication introduces another level of complexity regarding the protection of UNCLASSIFIED information. It's based on a subjective determination by a federal agency that the unclassified data is related to a "critical program or high value asset". This essentially creates another data classification type which, in turn, requires additional controls. Rationale: NIST 800-171 was created to provide "... agencies with recommended security requirements for protecting the confidentiality of CUI when the information is resident in nonfederal systems and organizations". Arguably, the biggest threat to that information is APT entities. Those controls are an adequate baseline. Many of the NIST 800-171B controls are equivalent to best business practices, while others are more "state of the art" and not achievable by average defense industrial base companies. Implementation of these demonstrates a higher cyber program maturity and should be used in evaluation under the emerging CMMC Program, not as part of an inflexible set of additional controls mandated by a subjective determination.	Abandon publication of NIST 800-171B and transition the controls into the evaluation criteria being developed under the Cyber Maturity Model Cerification (CMMC) Program.

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