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

Comment Template for
Initial Public Draft NIST SP 800-171B

Please submit responses to:
sec-cert@nist.gov by August 2, 2019

#	Organization Name	Submitted By	Type*	Page #^	Starting Line #^	Ending Line #	Section #	Comment (Include rationale for comment)^	Suggested Change^
1	Beryllium InfoSec Collaborative	Benjamin D. Brooks, CISSP EMBA	E	vii	152	153	N/A	This text box is good information, and a welcome reference. However, based upon experience with contractors and subcontractos to the DOD, most of whom are significatnly lacking in their information protections, we recommend more prescriptive guidance surroudning the adoption of the NIST CSF.	"Should an organization not have other or commensurate information security programs in place for holistic information protection, it is highly recommended that the organization consider adoption of the NIST CSF, as appropriate, in conjunction with the controls listed in Appendix D."
2	Beryllium InfoSec Collaborative	Benjamin D. Brooks, CISSP EMBA	G	2	224	226	Introduction	The use of the phrase, "the Advanced Persistent Threat" suggests a singular entity to which/ whom is given a title. Instead consider helping readers who may not be well versed in threat actors, in understanding that an APT could be a group or singular person but most importantly, that APTs are not limited to one organization or entity.	Consider, "... are potential targets for threat actors classified as an "Advanced Persistent Threat". An APT is an adversary or adversarial group...". Additionally, it is grammatically more appropriate to use human pronouns, as an APT consists of people, not objects or animals; consider the use of "they" instead of "it" when referring to APts.

#	Organization Name	Submitted By	Type*	Page #^	Starting Line #^	Ending Line #	Section #	Comment (Include rationale for comment)^	Suggested Change^
3	Beryllium InfoSec Collaborative	Benjamin D. Brooks, CISSP EMBA	E	11	458	468	Limiting the Scope of The Enhanced Security Requirements	Many organizations both large and small claim difficulty in identifying applicability of the SP 800-171. It would be wise to move this note of applicability earlier in the document.	To help readers understand the applicability of this document to their organization (or not), consider moving this text block to the end of Section 1.1: Purpose and Applicability.
4	Beryllium InfoSec Collaborative	Benjamin D. Brooks, CISSP EMBA	G	6	330	331	2.2	Advanced Persistent Threat is fully spelled out again, as if being first introduced in the document with (APT) at the end of the sentence.	Consider using the fully spelled out term or the acronym, alone.
5	Beryllium InfoSec Collaborative	Benjamin D. Brooks, CISSP EMBA	E	8	368	368	The Requirements	Advanced Persistent Threat is fully spelled out again, as if being first introduced in the document with (APT) at the end of the sentence.	Consider using the fully spelled out term or the acronym, alone.

#	Organization Name	Submitted By	Type*	Page #^	Starting Line #^	Ending Line #	Section #	Comment (Include rationale for comment)^	Suggested Change^
6	Beryllium InfoSec Collaborative	Benjamin D. Brooks, CISSP EMBA	T	14	541	543	3.2 Training and Awareness	It has been our experience that the majority of the target audience does not understand that all parties of an organization must be made cognizant of social engineering threats across the entire organization. Often the easiest persons to social engineer are not the ones who consider themselves part of the defense of the organization.	All persons in the organization should be made aware of the threat of social engineering as all members are potentially targets or must be able to resist social engineering attempts. Therefore we recommend it be made explicitly clear that this requirement (and others surrounding general user training) is applicable across the entire organization, not just IT professionals or those that are designated "CUI Handlers".

#	Organization Name	Submitted By	Type*	Page #^	Starting Line #^	Ending Line #	Section #	Comment (Include rationale for comment)^	Suggested Change^
7	Beryllium InfoSec Collaborative	Benjamin D. Brooks, CISSP EMBA	T	23	709	722	3.9 Personnel Security	While the NIST 800-53 does not prescribe the periodicity for assessing and reassessing personnel trustworthiness for good reason, NIST 800-171B should have a prescribed baseline recommended periodicity for conducting personnel screenings.	Recommend that the following verbiage be included. "Personnel screenings should be initiated before hire and at least once every 7 years of employment thereafter. Additionally, any change in personnel status that would bring into question an employee's trustworthiness should be reported immediately to the organizational security program manager."
8	Beryllium InfoSec Collaborative	Benjamin D. Brooks, CISSP EMBA	T	26-27	818	827	3.11 Risk Assessment	Many organizations do not understand the scope of this control, thinking it referes to raw materials sourcing, vice computer systems.	Recommend the inclusion of the following statement at the beginning of the Discussion: "This control applies to the acquisition of IT and OT systems, their parts, servicing, and maintenance."

#	Organization Name	Submitted By	Type*	Page #^	Starting Line #^	Ending Line #	Section #	Comment (Include rationale for comment)^	Suggested Change^
9	Beryllium InfoSec Collaborative	Benjamin D. Brooks, CISSP EMBA	G	28	847	874	3.12 Security Assessment	The description is an excellent inclusion for those organizations that may not have sufficient experience or knowledge of penetration testing.	
10	Beryllium InfoSec Collaborative	Benjamin D. Brooks, CISSP EMBA	E	43	N/A	N/A	Glossary	Cloud Computing is not defined in the glossary though it is referenced in the document. It has been our experience that many SMB's do not clearly understand cloud computing. The definition may be a helpful inclusion.	Recommend the inclusion of NIST's definition of "Cloud Computing" in the glossary.