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

Please submit responses to:
sec-cert@nist.gov by July 19, 2019

#	Organization Name	Submitted By	Type*	Page #^	Starting Line #^	Ending Line #	Section #	Comment (Include rationale for comment)^	Suggested Change^
1	HDR	L. Sisco	G	2	243	259	1.1	Very hard to audit and ensure proper controls if there is no distinguishable marking or special handling instructions on the electronic (or hardcopy) documents that require these enhanced security requirements.	Recommend that the CUI Program consider incorporating some type of additional marking or dissemination control that makes it clear that a document.
2	HDR	L. Sisco	G	23	707	722	3.9.1.e	The enhanced trustworthiness requirement is very vague. This isn't something required for organizations to do for personnel with actual security clearances. Yes there is a periodic background investigation but that happens every 5 years or more.	Recommend providing specific guidance as to what exactly is the standard or minimum requirement to meet the intent.

3	HDR	L. Sisco	G	34	1104	1136	3.14.4.e	The requirement to refresh twice annually is a very burdensome and expensive requirement. One might argue that if we think that information is so important to protect that it warrants this level of effort and expense that it probably should be classified and afforded the protection of a classified system.	Recommend removing this requirement completely.
4	HDR	L. Sisco	G	20	659	695	3.6.1.e & 3.6.2.e	This requirement to maintain a security operations center (SOC) and a cyber incident response team (CIRT) will be very challenging for small and medium sized businesses to meet.	Consider removing this requirement or relaxing it. For example; the intent can be met if a business is using an external provider that provides an equivalent level of service.

5	HDR	L. Sisco	G	N/A	N/A	N/A	N/A	A comment on the overall concept of this publication; similar to comment #3, shouldn't we consider information that is susceptible to the APT as classified if its intrinsic value is deemed that critical? Outwardly, it seems like we are implementing a lot of additional requirements to protect CUI that is now considered to have a need for even more protection. Sounds like it is starting to meet the basic definition of classified material if it is so important that we have to take all these steps to protect it.	