#	Organization Name	Submitted By	Type	Page #	Starting Line #	Ending Line #	Section #	Comment	Suggested Change
1	CNA	Carey Carter	E	3	251	253	1.1 - Purpose and Applicability	Where do we find the applicable critical programs or high value assets to determine if we must meet these requirements? More clarity needed on CPI and HVA.	Modify to include location of list or how to determine if organization is required to follow enhanced requirements.
2	CNA	Carey Carter	G	3	256	259	1.1 - Purpose and Applicability	Are all the requirements meant to be used or will the contracting officer determine the applicable set of requirements? If the latter, what training and guidance will contracting officers be given for this determination?	Clarification or responses to questions
3	CNA	Carey Carter	G	6	320	322	2.1 - Basic Assumptions	Does this mean that we can use alternate controls other than the ones defined? Who determines if the alternate controls are acceptable?	Clarification or responses to questions
4	CNA	Carey Carter	T	8	389	389	3 - The Requirements	Storage is mentioned in the requirements from a standpoint of ensuring the CUI data meets the retention, etc. of that data but the limiting of persistent storage is not mentioned. An example of this would be: are endpoints allowed to have hard drives?	Clarification or responses to questions
5	CNA	Carey Carter	T	12	471	482	3.1.1e - Access Control	Would having all privileged accounts be managed in a privileged account manager solution and those accounts be approved by a second party (i.e. manager) before its use meet this requirement? This would be an authorization for a task not by specific command.	Clarification or response to question
6	CNA	Carey Carter	G	18	621	640	3.5.2e - Identification and Authentication	Definition of complex account management needs to be included. There is one example given in the NIST discussion.	Include definition of complex account management
7	CNA	Carey Carter	G	23	707	722	3.9.1e - Personnel Security	Define the specifications of the enhanced personnel screening. Define the specifications of on-going enhanced personnel screening. What artifacts are required for the initial screening and the on-going screening? Would a security clearance meet the intent of the enhanced personnel screening requirement.	Include definition of enhanced personnel screening, specification of on-going enhanced personnel screening, and definition of required artifacts for both the initial and on-going screening.
8	CNA	Carey Carter	G	26	816	827	3.11.6e - Risk Assessment	Define assessment of supply chain. Is there a standard to be followed? What artifacts are required?	Include definition of assessment of supply chain to include a followed standard and required artifacts from assessment.
9	CNA	Carey Carter	T	29	877	909	3.13.1e - System and Communications Protection	This needs clarification. The first half of the NIST discussion centers around having a heterogeneous environment. If that is the case what percentages of hardware, operating systems, databases, web servers, etc. are allowed to be from a specific vendor or is the intent to have diversity of security tools?	Clarification or responses to questions

#	Organization Name	Submitted By	Type	Page #	Starting Line #	Ending Line #	Section #	Comment	Suggested Change
10	CNA	Carey Carter	T	29	910	955	3.13.2e - System and Communications Protection	The requirement seems to imply that it is only concerned with systems and system components. The NIST discussion goes into storage locations, network changes, etc. This requirement needs to be clarified on where these changes are to made as well as to what level the changes need to be made. When we talk about moving target defense on systems we generally see tools that modify the memory footprint of processes thus causing the attacker to modify the in-memory attack exploit before running which is assuming that the attacker is able to do that before the randomness comes in and changes it. Does one of these tools meet this requirement or do we need to also get a solution for the network layer and other items on the attack surface? This manual is written under the assumption of an APT on the network, if they are already on the network and have access to monitor the network then they would see the changes made to the network. Do we need a solution that constantly changes the location of storage used by the servers and endpoints? When the NIST discussion refers to non-persistence it would seem like the semi-annual refresh of systems would not be frequent enough to meet this requirement. If we step away from moving target defense, could adding random honeypots or honeynets meet this requirement?	Clarification or responses to questions
11	CNA	Carey Carter	G	30	956	975	3.13.3e - System and Communications Protection	The requirement states a combination of three items but uses an or. Does this mean that only 2 of the items are needed? Is adding a honeypot/honeynet with disinformation enough to meet this requirement? Does every system/process require tainting and/or misdirection? If a honeypot is used is there an adequate level of deception that needs to be met?	Clarification or responses to questions
12	CNA	Carey Carter	E	33	1020	1044	3.14.1e - System and Information Integrity	This requirement contradicts the requirements for moving target defense. If we are constantly changing our applications for that requirement, our application whitelisting and/or file integrity monitoring solutions are unable to determine if the random file is trusted.	Provide clarification to perceived contradiction in requirements
13	CNA	Carey Carter	E	33	1045	1067	3.14.2e - System and Information Integrity	The NIST discussion implies the usage of a SIEM to gather information from various locations is required but the requirement, as written, does not imply that.	Modify requirements to match discussion or vice versa
14	CNA	Carey Carter	T	34	1104	1136	3.14.4e - System and Information Integrity	This requirement is stated to be done two times a year which would leave any APT six months to operate which seems like more than enough time to get what they want. Does this include all network devices, storage devices, security devices, etc.? When rebuilding an application on a server it would be necessary to restore application data that was in use prior to the rebuild, is this allowed? If the systems are whitelisted is this requirement even needed? We are concerned that this control will lead to significant operational impact and expense.	Clarification or responses to questions

#	Organization Name	Submitted By	Type	Page #	Starting Line #	Ending Line #	Section #	Comment	Suggested Change
15	CNA	Carey Carter	G	35	1137	1151	3.14.5e - System and Information Integrity	The control mentions federal records retention policies and disposition schedules. It should also reference, or make allowances for contractual requirements. As an FFRDC, we are expected and our contract allows us to maintain data repositories to support longitudinal research studies.	Clarification or responses to questions
16	CNA	Carey Carter	E, G	2	244	259	1.1 - Purpose and Applicability	Clarify: "The recommendations apply only to the components of nonfederal systems that process, store, or transmit CUI contained in a critical program or high value asset or that provide protection for such components." Explicitly word document to prevent contracting officers from declaring all of its contractors supporting critical programs or high value assets to meet all requirements for all organizational systems and clarify the costs allowable under the contract.	Explicitly word document to prevent contracting officers from declaring all of its contractors supporting critical programs or high value assets to meet all requirements for all organizational systems and clarify the costs allowable under the contract.
17	CNA	Carey Carter	E, G, T	All	All	All	General	CMMC is coming out soon; please defer this document and the FAR until CMMC is released to avoid confusion. It will be important to reconcile the requirements of 800-171B and CMMC.	Defer this document and the FAR until CMMC is released to avoid confusion
18	CNA	Carey Carter	E, G, T	12	483	490	3.1.2e - Access Control	Our assumption is that the word "provisioned" is intended to allow for the use of cloud services where the organization itself does not own the hardware but provisions the services. Is that correct?	Clarification to include all questions.
19	CNA	Carey Carter	E	14	522	537	3.2.1e - Awareness and Training	Who defines "when there are significant changes to the threat?"	Clarification to include question
20	CNA	Carey Carter	E, G, T	16	557	572	3.4.1e - Configuration Management	Does term "system components" include things like Ruby Gem or Python Module? Do you need MS patches cached locally? Is this a source code repository mirror? - Is this just operating systems or enterprise software? - How far down into the system do you go into the hardware and system components? - Is expectation to track firmware updates on all servers, computers and printers which process, store or come into contact with CUI / CDI data? - Define "trusted and authoritative source"	Clarification to include all questions
21	CNA	Carey Carter	E, G, T	18	641	655	3.5.3e - Identification and Authentication	Is the intent NAC with posture assessment?	Clarification to include all questions
22	CNA	Carey Carter	E, G, T	20	659	677	3.6.1e - Incident Response	Need to de-conflict with 3.1.2 wrt using third-party SOC providers (e.g. MSSP will deploy sensors in the enclave to provide SOC services, is that ok?)	Clarification to include all questions and contradiction instances of a 3rd party SOC

#	Organization Name	Submitted By	Type	Page #	Starting Line #	Ending Line #	Section #	Comment	Suggested Change
23	CNA	Carey Carter	E, G, T	25	750	771	3.11.2e - Personnel Security	- Can Hunt team be an outsourced option? If yes, please provide as example. - How often do you need to perform threat hunting - What artifacts of evidence do you need to provide to prove threat hunting? Concern: High Cost especially for small business	Clarification to include all questions and concern for small business
24	CNA	Carey Carter	E, G, T	25	772	786	3.11.3e - Personnel Security	- Does control explicitly require the use of artificial intelligence for compliance? Concern: High Cost	Clarification to include question and concern
25	CNA	Carey Carter	E, G, T	26	816	827	3.11.6e - Personnel Security	To be effective, this will require the government to share intel on supply chain threats.	Clarification to include all questions and concern of practicality
26	CNA	Carey Carter	E, G, T	27	828	845	3.11.7e - Personnel Security	Is the expectation to create a supply chain department focused on this? Is this just a process to address 3.11.6e? Scope and depth both need to be defined. Concern: - High cost (potential) depending on scope and implementation	Clarification to include all questions and concern of practicality
27	CNA	Carey Carter	E, G, T	29	910	955	3.13.2e - System and Communications Protection	This control in conjunction with the configuration management requirements may create a significant workload to be both random and fully baselined and documented. This will have significant operation impacts and costs.	Clarification to include all questions