#	Organization Name	Submitted By	Type*	Page #^	Starting Line #^	Ending Line #	Section #	Comment (Include rationale for comment)^	Suggested Change^
1	Leidos	Jonathan Jowers / Craig Meyer	G	12	471	482	3.1.1e Employ dual authorization to execute critical or sensitive system and organizational operations.	Can this be clarified to state if this is intended for each action, or for a user to gain initial access. E.g., will users be required to get approval to obtain privileges, through authorization of two individuals? Is this not 2FA and MFA OR is this two person control? Does this mean two people are required when executing certain commands, operations, or functions? Serial or in parallel. I don't see small contractors as being able to	
2	Leidos	Jonathan Jowers / Bill Lewandowski / Craig Meyer	G	12	483	490	3.1.2e Restrict access to systems and system components to only those information resources that are owned, provisioned, or issued by the organization.	Does BYOD end with this control? Is that the intention? Does this mean cloud services can't be used. 800-53 has options to restrict or prohibit external systems. I think this allows us to use Cloud as we would be “provisioning” and “Issuing” but would like to hear a better explanation/definition.	It is not clear what applying this control would should mean in many circumstances; remove the control unless the meaning of it can be clarified.
3	Leidos	Jonathan Jowers / Bill Lewandowski / Craig Meyer	G	12-13	491	518	3.1.3e Employ secure information transfer solutions to control information flows between security domains on connected systems.	Is the intent of this control to know where all data is, even in a cloud environment? Also, what are the details in the SC-46 Cross Domain Policy Enforcement? Do we have a definition of “Security Domain”? What are the minimum requirements? It appears that this control is derived from 800-53 AC-4. However, it doesn't map to any specific	The meaning is not clear for this control, suggest removal unless the meaning of the controlc an be verified.
4	Leidos	Jonathan Jowers / Bill Lewandowski / Craig Meyer	G	16	557	569	3.4.1e Establish and maintain an authoritative source and repository to provide a trusted source and accountability for approved and implemented system components.	What are the differences in this control compared to NIST SP 800-171r1 3.4.1 and 3.4.3 controls?	
5	Leidos	Jonathan Jowers / Bill Lewandowski / Craig Meyer	G	16-17	589	603	3.4.3e Employ automated discovery and management tools to maintain an up-to-date, complete, accurate, and readily available inventory of system components.	Is the intent to use advanced tools to know everything (definition of what? Managed and unmanaged devices) connected to IS network?	
6	Leidos	Jonathan Jowers / Bill Lewandowski / Craig Meyer	G	18	607	620	3.5.1e Identify and authenticate systems and system components before establishing a network connection using bidirectional authentication that is cryptographically-based and replay resistant.	Does this control include operating systems other than Windows? What are the ramifications (Clarification) of "Before establishing a network connection"?	

#	Organization Name	Submitted By	Type*	Page #^	Starting Line #^	Ending Line #	Section #	Comment (Include rationale for comment)^	Suggested Change^
7	Leidos		G	18	621	640	3.5.2e Employ password managers for the generation, rotation, and management of passwords for systems and system components that do not support multifactor authentication or complex account management.	Clarify the requirement, rather than a solution? Reads like the solution.	
8	Leidos	Jonathan Jowers / Craig Meyer	G	23	707	722	3.9.1e Conduct enhanced personnel screening (vetting) for individual trustworthiness and reassess individual trustworthiness on an ongoing basis.	What are the enhancements from current screening, criminal background checks and termination processes already required?	
9	Leidos	Jonathan Jowers / Bill Lewandowski / Craig Meyer	G	23-24	723	729	3.9.2e Ensure that organizational systems are protected whenever adverse information develops regarding the trustworthiness of individuals with access to CUI.	Define adverse information? What is the enhancement from existing data protection & monitoring controls?	
10	Leidos	Jonathan Jowers / Bill Lewandowski / Craig Meyer	G	25	737	749	3.11.1e Employ threat intelligence to inform the development of the system and security architectures, selection of security controls, monitoring, threat hunting, and response and recovery activities.	Clarify difference to control 3.14.3?	
11	Leidos	Jonathan Jowers / Bill Lewandowski / Craig Meyer	G	25-26	772	786	3.11.3e Employ advanced automation and analytics capabilities to predict and identify risks to organizations, systems, or system components.	Is this an enhamcement to Security Operations Center functions?	
12	Leidos	Jonathan Jowers / Craig Meyer	G	26-27	805	815	3.11.5e Assess the effectiveness of security solutions at least annually to address anticipated risk to the system and the organization based on current and accumulated threat intelligence.	Is the intent of this control to provide a prescriptive Organization Define Value (ODV) for control reviews?	Suggest changing the "at least annually" statement to "organizationally defined frequency.

#	Organization Name	Submitted By	Type*	Page #^	Starting Line #^	Ending Line #	Section #	Comment (Include rationale for comment)^	Suggested Change^
13	Leidos	Jonathan Jowers / Craig Meyer	G	28	849	872	3.12.1e Conduct penetration testing at least annually, leveraging automated scanning tools and ad hoc tests using human experts.	Is the intent of this control to provide a prescriptive Organization Define Value (ODV) for control reviews?	Suggest changing the "at least annually" statement to "organizationally defined frequency.
14	Leidos	Jonathan Jowers / Craig Meyer	G	29	906		3.13.1e Employ diverse system components to reduce the extent of malicious code propagation.	Will a document like NIST SP 800-171A be created to provide guidance on all controls? This control is very broad and has many requirements. What are "diverse system components"? The irony here is that we try to standardize on platforms in order to scale compliance to all of hte existing controls. If we purposly make our	Suggest removing this control because it works agaist our ability to create robust secured platforms. This would be especially true for smaller companies.
15	Leidos	Jonathan Jowers / Craig Meyer	G	29-30	910	952	3.13.2e Disrupt the attack surface of organizational systems and system components through unpredictability, moving target defense, or non-persistence.	Is this control intended to "edge" towards national security level protections? Are contractors required to implement deception techinques? How will they be measured for effectiveness? Like the previous control this control would make it harder for us to maintain a properly secured	Suggest removing this control because it works agaist our ability to create robust secured platforms. This would be especially true for smaller companies.
16	Leidos	Jonathan Jowers / Craig Meyer	G	30-31	956	974	3.13.3e Employ technical and procedural means through a combination of misdirection, tainting, or disinformation to confuse and mislead adversaries.	Will a document like NIST SP 800-171A be created to provide guidance on all controls? This control is very broad and has many requirements.	
17	Leidos	Jonathan Jowers / Craig Meyer	G	33	1020	1044	3.14.1e Employ roots of trust, formal verification, or cryptographic signatures to verify the integrity and correctness of security critical or essential software.	What would be an example of an audit plan to address this control?	
18	Leidos	Jonathan Jowers / Craig Meyer	G	34	1068	1102	3.14.3e Ensure that Internet of Things (IoT), Operational Technology (OT), and Industrial Internet of Things (IIoT) systems, components, and devices are compliant with the security requirements imposed on organizational systems or are isolated in purpose- specific networks.	Is this control requiring combinations (joining) of 24/7 Security Operations Center monitoring, anti-virus, and data loss prevention? Which requirements STIG,etc.? What are the configurations control standards?	

#	Organization Name	Submitted By	Type*	Page #^	Starting Line #^	Ending Line #	Section #	Comment (Include rationale for comment)^	Suggested Change^
19	Leidos	Jonathan Jowers / Craig Meyer	G	34-35	1104	1136	3.14.4e Refresh organizational systems and system components from a known, trusted state at least twice annually.	Will a document like NIST SP 800-171A be created to provide guidance on all controls? This control is very broad and has many requirements. Of all the controls 3.14.4e is the most concerning both technically and cost especially if it takes in to account 'all' devices to include Windows, Mac, LINUX, servers (of all flavors), switches, routers, firewalls, etc. This could be a full time staff and all the risk it introduces in to operations. What a management and risk nightmare. Unless I am misunderstanding this control, this control does not scale. It sounds like this control is suggesting we wipe away software installations and configurations and start over twice a year.	Ideally; remove this control because it introduces risk and unecessary work that could be used elsewhere to better secure the envrionment. At a minimum, change "twice annually" to "organizationally defined interval"
20	Leidos	Jonathan Jowers / Bill Lewandowski/ Craig Meyer	G	35-36	1137	1151	3.14.5e Conduct periodic reviews of persistent organizational storage locations and purge CUI that is no longer needed consistent with federal records retention policies and disposition schedules.	Is this only Policy and procedure only? What is the intended enhancement? Is there a definition of 'persistent organizational storage'? Destruction or other? (I.e., Key, hardware, sanitation) Is there a definition of 'persistent organizational storage'?	
21	Leidos	Jonathan Jowers / Bill Lewandowski	G	36	1152	1167	3.14.6e Use threat indicator information relevant to the information and systems being protected and effective mitigations obtained from external organizations to inform intrusion detection and threat hunting.	Clarify difference to control 3.14.1e? Recommendations of which services to use? E.g., US-CERT, NDISAC, DSIE, McAfee?	