#	Organization Name	Submitted By	Type*	Page #^	Starting Line #^	Ending Line #	Section #	Comment (Include rationale for comment)^	Suggested Change^
1	Integrated Security Solutions	Dianne Gallatin	G	12	3	14	3.1	3.1.1e: Employ dual authorization to execute critical or sensitive system and organizational operations. - Clarification: Need clarification of intent/definition of "critical or sensitive system and organizational operations". If too broadly defined, the impact is: - - Execution of privileged commands are required daily in order to implement, maintain, and support information systems. If 3.1.1e is mandated by a federal agency in a contract, grant, or other agreement, will guidance be provided to determine the extent to where this requirement will apply? Requiring dual authorization for the execution of privileged commands may require significant additional personnel resources. - Can this requirement be solved through monitoring and correlating changes detected in the environment with change management records, so long as a technical review of the change is part of the change management process?	

#	Organization Name	Submitted By	Type*	Page #^	Starting Line #^	Ending Line #	Section #	Comment (Include rationale for comment)^	Suggested Change^
2	Integrated Security Solutions	Dianne Gallatin	G	12	15	22	3.1	3.1.2e: Restrict access to systems and system components to only those information resources that are owned, provisioned, or issued by the organization. - Clarification: does 3.1.2e apply to mobile devices (ex. smart phones and tablets), or is BYOD acceptable for email access, so long as encrypted containerization is used and the organization maintains the ability to remote wipe encrypted containers from mobile devices?	

#	Organization Name	Submitted By	Type*	Page #^	Starting Line #^	Ending Line #	Section #	Comment (Include rationale for comment)^	Suggested Change^
3	Integrated Security Solutions	Dianne Gallatin	G	29	36	47	3.13	3.13.2.e: Disrupt the attack surface of organizational systems and system components through unpredictability, moving target defense, or non-persistence. - The guidance provided (ex. moving target defense and non-persistence) can significantly impact business operations and reduce the level of agility needed to support the federal agency's mission. Does a layered approach mitigate the risk? For example, if the organization additionally has a robust Insider Threat program that automatically tracks and reports on primary risk indicators, will disrupting the attack surface at the perimeter suffice? - Are Network Access Control and Zero Trust (Software-Defined Perimeter) solutions acceptable as either equivalent or mitigating controls for this requirement?	
4	Integrated Security Solutions	Dianne Gallatin	G	34	41	48	3.14	3.14.4e: Refresh organizational systems and system components from a known, trusted state at least twice annually. - The frequency of a system refresh should be determined by the system's risk profile. Requiring a refresh at least twice annually may cause significant impact to business operations and may impact the organization's ability to support the federal agency's mission.	