#	Organization Name	Submitted By	Type*	Page #^	Starting Line #^	Ending Line #	Section #	Comment (Include rationale for comment)^	Suggested Change^
	The Pennsylvania State University	Joseph Gridley	G	20	659	674	3.6.1e	The requirement for a 24/7 SOC staffed by personnel creates prohibitive operational cost, especially with regard to federally funded research projects with Universities. The objective of 24/7 ongoing monitoring, including detection, alerting, and response, can be accomplished through the use of automated tools. Organizations should be allowed to tailor their approach to meet the objective of ongoing monitoring using their own best-fit combination of technology and personnel rather than a specific requirement to use human beings. Note that this change would also be consistent with industry trends leaning toward automation and technology tools in place of additional human resource investment.	is the focal point for security operations and computer network defense for an organization. The purpose of the SOC is to defend and monitor an organization's systems and networks (i.e., cyber infrastructure) on an ongoing basis. The SOC is also responsible for detecting, analyzing, and responding to cybersecurity incidents in a timely manner. The SOC is staffed with skilled technical and operational personnel (e.g., security analysts, incident response personnel, systems security engineers); operates 24 hours per day, seven days per week; and implements technical, management, and operational controls (including monitoring, scanning, and forensics tools) to monitor, fuse, correlate, analyze, and respond to threat and security-relevant event data from multiple sources. Sources include perimeter defenses, network devices (e.g.,