#	Organization	Commentor	Type	Page #	Line #	Section	Comment (Include rationale for comment)	Suggested change
	SCE		E	22		Security Continuous Monitoring (CM)	Security Continuous Monitoring should include "Prevent"	Consider: The information system and assets are monitored to identify, detect and prevent cybersecurity anomalies and events
	SCE		E	14		Business Environment (BE)	We should include activity related to alignment with business needs.	Add "Alignment with Business need"
	SCE		E	15		Governance ID. GV-2	"Information security roles & responsibility are coordinated….?" Incomplete sentence	Completed as "Information Security roles and responsibilities are coordinated and aligned with corporate organization structure"
	SCE		E	15		Governance ID. G-4	Risks are not just addressed but are managed too	Governance and risk management process address and manage cybersecurity risks
	SCE		E	16		Risk Assessment ID.RA 6	Include activity related to remediation of vulnerability	Develop and execute remediation plan for identified vulnerability
	SCE		E	16		Risk Management Strategy ID.RM-1	This looks incomplete: Risk management processes are managed and agreed to….?	Consider "Risk management processes are managed and agreed to by all organizational stakeholders"
	SCE		E	17		Access Control PR.AC-3	Remote access is managed. Just management is not enough.	Consider: Remote access is managed and controlled
	SCE		E	17		Access Control PR.AC-4	Include "controlled."	Consider: Access permissions are managed and controlled
	SCE		E	17		Awareness and Training PR.AT-1	Who are considered "General Users"	Consider: "Users without elevated or privileged access"
	SCE		E	17		Awareness and Training PR.AT-2	Even privileged users needs to be trained	Consider: Privileged users understand roles & responsibilities and are trained
	SCE		E	14		Identify ID.BE-1	Sentence is broken and unclear	Consider "The organization's role in the supply chain is identified and communicated"

	SCE		E	16		Protect PR.AC-1	Need to include 'processes' in the statement. Category statement identifies processes as part of access controls but this statement only addresses users and devices	Change wording to a statement similar to: Identities and credentials are managed for authorized devices, users, and processes (including information systems).
	SCE		E	17		Protect PR.AC-3	Informative references should include AC-18 in the NIST SP 800-53 Rev 4 line item. Wireless access is related to Remote Access as well as use of Mobile Devices.	* NIST SP 800-53 Rev 4 AC-17, AC-18, AC-19, AC-20
	SCE		E	20		Protect PR.IP-8	Sentence needs to include the words "approved" and "authorized." This will better align the subcategory with wording within NIST 800-53 AC-21	Change wording to a statement similar to: Information sharing occurs with appropriate approved and authorized parties
	SCE		E	21		Protect PR.PT-3	The reference to NIST SP 800-53 CM-7 needs to be more completely referenced.	Include "and related controls" when referencing NIST 800-XX Controls
	SCE		E	21		Protect PR.PT-4	Informative reference NIST 800-53 AC-18 is out of place and does not align with the Subcategory statement	Remove NIST 800-53 AC-18 reference and replace with NIST 800-53 CM-7
	SCE		E	23		Detect DE.CM-7	Statement is vague and unclear. "Unauthorized resources are monitored."	Change wording to a statement similar to: "Monitoring processes are implemented to detect unauthorized access to resources"
	SCE		E	24		Respond RS.PL-1	'Implementing' a response plan during an event seems to be a rather backward approach. The response plan should be executed during an event and not simply implemented.	Change to: Response plan is executed during an event
	SCE		G				NIST 800-53 controls are extendable to other related controls	Within Informative References, include "and related controls" when referencing NIST-800-53 controls, where applicable

	SCE		G	3		1.2	Establishing a Risk Management program is a key component required to successfully implement the framework. While this section provides a good overview of a risk-based approach at the organizational level, more clarity is required by linking the main components of the framework: Tiers, Profiles and Core (Lines 699-701). The Framework needs to clarify the scope, and how to evaluate risk and apply the risk within the Framework. The focus should be on risks relevant to critical infrastructure. A broad definition could dilute valuable resources making the Framework less effective. Clearly defining the scope can assist in how the risk management process will be used.	Provide an implementation guide that clarifies the framework components and their interdependencies with the risk management process, and how an organization should focus on risks as the risks relate to other government led cybersecurity programs such as the NIPP
	SCE		G	41	677	Appendix D	"Complement rather than conflict with current regulatory authorities" needs to be enhanced with more guidance. If state legislatures and regulators begin independently addressing cybersecurity concerns inconsistent approaches, the lack of cohesion could actually reduce our overall defenses.	Provide guidance to state legislatures and regulators regarding how to view the framework and their role with respect to the Framework. Engage sector agencies to develop.
	SCE		G	42	721	Appendix E	The definition of Personal Identifiable Information (PII) varies from state-to-state. The framework should not create its own definition.	Cite external state approved references in the Glossary where possible and use an example of a definition that is specific and clear.
	SCE		G	3	150	1.1	Implementation Tiers do not have a progression path	Tiers should have a progression path that meets certain objectives in order to reach a more mature tier

	SCE						The term "adoption" needs clarification	• The December 4, 2013 “Update on the Development of the Cybersecurity Framework” stated that the discussion at the Raleigh Workshop resulted in a “general consensus” for a particular definition of the Framework “adoption.” However, it is unclear what general consensus was reached, other than a concern that the term was not well defined