#	Organization	Commentor	Type	Page #	Line #	Section	Comment (Include rationale for comment)	Suggested change
1			G			entire document	The Preliminary Framework is a well-equipped and organized "tool box" of cybersecurity controls and best practices, but it lacks guidance on how to choose among all the available tools. It is also a flat collection of controls and practices, with no prioritization among them. Continuing with the tool box analogy, all the wrenches, screwdrivers, drill bits, and hammers are nicely organized and categorized, but the user has no idea when to use a flat blade screwdriver versus a Phillips head screwdriver or when to use a wrench versus locking pliers.	Consider identifying a few standard sets of security controls (e.g., "basic", "mid-level", and "luxury") with increasing levels of robustness and commensurate increasing costs.
2			G			entire document	Cybersecurity-aware organizations, such as large financial institutions and large utilities, already implement the controls and follow the best practices described in the Cybersecurity Framework. The organizations that stand to benefit the most from the Framework are those that are new to cybersecurity, especially smaller organizations with limited resources. Yet the Preliminary Framework fails to provide detailed guidance on how to implement it. For example, it glosses over the importance of understanding the threats and risks that your system faces, and seems to jump right to a detailed list of security standards and controls. But the controls that an organization needs to implement should be determined by the threats against which their systems need to be protected. One size does not fit all. Users of the Framework will need guidance on how to tailor the set of security controls to their particular environment and situation.	Develop guidelines for mapping threat scenarios and risk management strategies to specific sets of security controls. Provide guidance on how to develop a cybersecurity program that takes into account the tradeoffs between costs and benefits.

3			G	1	71	1	Consider including an overall critical infrastructure conceptual layered view that shows how critical infrastructure ties to other layers (e.g., Power, Gas, Water, Telecommunication…)	
4			G	1	79	1	The scope should not be limited to information technology, but should be broadened to include supporting communication technology. This line should reference information and communication technology (ICT), rather than just information technology (IT).	"Each sector performs critical functions that are supported by information and communication technology (ICT)…"
5			G	2	111	1.1	The Preliminary Framework frequently claims to be "risk-based," but it contains very little discussion of the risk assessment methodology, such as the need to identify and characterize cybersecurity threats.	
6			T	7	259	2.1	The description of the Core Function "Detect" does not mention the concept of auditing, which is an important Outcome Category. Although it may be part of the identified Outcomes, it should be explicitly mentioned, since it is a common category of security controls in many industry best practices.	
7			T	7	281	2.2	The concept of Framework Profiles is very useful, but the Preliminary Framework does not provide enough guidance on how an organization might develop a profile for their specific situation and threat environment. The key to implementing a robust cybersecurity program is defining the right Target Profile. The Preliminary Framework should include one or two example Profiles for different types of user organizations, such as a rural electric cooperative and a medium-sized bank.	Include examples of Target Profiles. Or consider a structure similar to that used in Department of Defense Instruction (DoDI) 8500.2, wherein specific security controls are selected based on the mission assurance category (MAC) and confidentiality level (CL) of the system. The higher the mission criticality of a system and the required level of confidentiality of the information it processes/stores, the more stringent the set of security controls it needs to implement.

8			G	9	321	2.4	The concept of Tiers is somewhat orthogonal to the purpose of the Framework and in conflict with the notion of Framework Profiles. How does a "desired" Tier map to a "target" Profile? The definitions of the Tiers sound more like assessment results than desired levels of rigor and sophistication in a risk management program. What organization would "desire" to be a Tier 1 organization?	Remove or rework the section describing the Implementation Tiers.
9			T	11	409	3.2	The recommended steps to using the Framework to create or improve a cybersecurity program are very useful, but they would be even more useful if an example or a case study were included to illustrate the process.	Include a case study to illustrate the process described in this section.
10			T	13	457	Appendix A	Appendix A identifies IA/security controls without explicitly identify the threats the controls protect against. IA controls should be selected based on the threats facing a system.	Add threat descriptions to be mitigated before mapping to IA Controls (i.e., Subcategories).
11			E	27	478-484	Appendix A	This material on the structure of the Framework and the identifiers for Functions and Categories should be moved to the beginning of Appendix A. It provides important information on how to interpret the various abbreviations and acronyms.	Move these lines and the table to the beginning of Appendix A.
12			G	28	485	Appendix B	Privacy is just one constraint on a cybersecurity program. There may be others, such as safety. Why does the Preliminary Framework explicitly address Privacy concerns?	Consider removing Appendix B or adding Appendices for other constraints on the implementation of a cybersecurity program.
13			T	39	619	Appendix C	Reference is made to "RS.CO" in Appendix B, but this Subcategory identifier is not used in Appendix B.	Better cross-referencing is needed between Appendix A and Appendix B.
14			T	42	686	Appendix E	The Glossary is missing some key terms and their definitions. For example, it needs to include definitions of "threat" and "vulnerability," two important factors in risk management.	Expand the Glossary to include missing cybersecurity terms/concepts.

15			T			Appendix A Alternative View	The Alternative View of Appendix A is too detailed and confusing, especially for audiences who are new to cybersecurity or who are not involved with the intimate details, such as executive-level managers.	Stick with the format of Appendix A as it is presented in the main Preliminary Cybersecurity Framework.