#	Organization	Page #	Line #	Section	Comment (Include rationale for comment)	Suggested change
1	SSA	i	11-12		**Does the Preliminary Framework adequately define outcomes that strengthen cybersecurity and support business?** Yes, the Framework defines outcomes that strengthen and support business, however, there are areas within the document that can be simplified and/or expanded (see suggested changes for specific sections).	Suggested Improvement: a) Provide a high-level description of the relationship between this framework and similar ones; b) Consolidate and/or simplify sections (e.g. subcategories) and c) Discuss System Development Life Cycle (SDLC) and continuous monitoring as it pertains to the development and implementation of the this Framework.
2	SSA	i	13		**Does the Preliminary Framework enable cost-effective implementation?** Organizations are encouraged to use existing risk-managing processes already defined and/or implemented, thus lowering the cost or keeping it at an acceptable level.	Suggested Improvement: Continue to make improvements towards consolidating and simplifying the information.
3	SSA	i	14		**Does the Preliminary Framework appropriately integrate cybersecurity risk into business risk?** Yes. A cybersecurity risk is a risk that can adversely affect the business (organization) and this framework has incorporated such risks and countermeasures (e.g. protecting PII, asset management, etc.)	Suggested Improvement: Expand on how this framework is incorporating cybersecurity risk into business risk.

4	SSA	i	15-16		**Does the Preliminary Framework provide the tools for senior executives and boards of directors to understand risks and mitigations at the appropriate level of detail?** Although the Profile captures enough information for the senior executives, it could also add information on current Tier and "target" Tier.	Suggested Improvement: Add the "Tiers" as a sub-component of "Profile" (see comment #15 for details)
5	SSA	i	17-18		**Does the Preliminary Framework provide sufficient guidance and resources to aid businesses of all sizes while maintaining flexibility?** According to the Preliminary Framework the organization's current risk tolerance, threat environment, legal and regulatory requirements, business/mission objectives and constrains ought to be taken into consideration, this indicates that no matter the size of the organization, the framework can be tailored.	Suggested Improvement: Provide more insight on the utilization of Framework for different business sizes and risk levels (low/moderate/high).

6	SSA	i	19-20		**Does the Preliminary Framework provide the right level of specificity and guidance for mitigating the impact of cybersecurity measures on privacy and civil liberties?** The description provided in the methodology section of this framework provides privacy and civil liberties that need to be taken into consideration when implementing and working to reduce cybersecurity risk; however, it did not address it in the "Business Environment" category.	Suggested Improvement: Include guidance on cybersecurity measures on privacy and civil liberties as it pertains to Business Environment.
7	SSA	i	21		**Does the Preliminary Framework express existing practices in a manner that allows for effective use?** It expresses existing practices in a manner that allows for effective use, and as stated, it can be scaled based on the business need and organization environment. However, there areas within the Framework that needs to be consolidated or/and simplified.	Suggested Improvement: Expand where there is more value to be added, like the Core and Profile sections. Limit the amount of information for Tiers implementation section or add a matrix providing a weight to each tier.

8	SSA	i	23-25		**Will the Preliminary as presented be inclusive of, and not disruptive to, effective cybersecurity practices in use today, including widely-used voluntary consensus standards that are not yet final?** The framework is intended to be complimentary of existing risk-based management tools and not replace any particular one; the proposed is flexible and scalable.	Suggested Improvements: There is nothing disruptive to a Framework that is voluntary in nature, in order to maintain the non-disruptive, and all inclusive approach continue to reference and line up the framework with similar frameworks and processes.
9	SSA	i	26		**Will the Preliminary as presented enable organizations to incorporate threat information?** The Framework can be tailored and the organization can incorporate threats that are unique to the organization's environment.	Suggested Improvement: Expand on specific guidance on how organizations can incorporate threat information within the proposed framework.
10	SSA	i	29		**Is the Preliminary Framework: presented at the right level of specificity?** Although the framework presents substantial information, there are sections within the document that can use a bit more clarity, for example, the target profile and the gap identification process.	Suggested Improvement: Refine the three (3) parts of the Framework (Core, Profile and Tiers) and suggest examples of outputs for each function subcategory.

11	SSA	i	30-31		**Is the Preliminary Framework: sufficiently clear on how the privacy and civil liberties methodology is integrated with the Framework Core?** It is not very clear why under Table 3: Methodology to Protect Privacy and Civil Liberties for a Cybersecurity Program, Business Environment (BE) is N/A, when the category is described as "**Business Environment (BE):** The organization's mission, objectives, stakeholders, and activities are understood and prioritized, and inform cybersecurity roles, responsibilities, and risk decisions." It appears based on the description that at a minimum the protection of Privacy and Civil Liberties are considerations in the realm of stakeholders, cybersecurity roles, responsibilities and risk decision.	Suggested Improvement: Identify and describe how privacy and civil liberties influences Business Environment. There are organizations in which privacy and civil liberties as part of the core of the organization mission, objectives, stakeholders and risk decisions.
12	SSA	1	74	1.0	"Due to the increasing pressures from external threats, organizations responsible for critical infrastructure need to have a consistent and iterative approach to identifying, assessing, and managing cybersecurity risk."	Suggested Improvement: Add to the verbiage "internal" threats. As seen in the media in recent months, the threat is both internal and external.

13	SSA	4	186-187	1.3	The order presented in this section, does not match the order presented in previous segments within the document. "Section 2 describes the Framework components: the Framework Core, the Tiers, and the Profiles."	Suggested Improvement: Maintain the same order previously provided, example: Core, Profile and Tiers.
14	SSA	9	322-331	2.4	The Framework Implementation Tiers should be a part of the Framework Profile. When an organization identifies the “current” Profile, it should include the “current’ Tier and the "Target" Profile should include a target implementation Tier.	Suggested Improvement: Add the "Tiers" as a sub-component of "Profile".
15	SSA	10	349	2.4	The wording Organizational-wide” appears to have deviated from previous citing of the word in the document (e.g. “Organization-wide”)	Suggested Improvement: Use "Organization-wide" where applicable in the document.
16	SSA	11	409	3.0	While step 1 through step 6 provide organizations with adequate level of description, adding “similar” activities or activities that aim at similar outcome/output is beneficial, thus increasing the Framework level of specificity and integration with similar frameworks.	Suggested Improvement: Add examples of risk-based activities, these can be activities already implemented or planned by the organization.

17	SSA	21	PR.PT-2	Appendix A	This appear to be a formatting error. Un-bold the leading "R" in "Removable."	Suggested Improvement: Un-bold the leading "R" in "Removable."
18	SSA	24	RS.PL	Appendix A	This appear to be a formatting error. RS.RP-1 should have been used instead of RS.PL-1.	Suggested Improvement: Use RS.RP-1 [Response Planning] and update the subcategory to reflect change.
19	SSA	25	RS.IM	Appendix A	Instead of two separate categories and subcategories, merge the "Improvements (IM)" category and subcategory from the “Respond (RS)” Function into the Response Planning (RP) category/subcategory.	Suggested Improvement: Incorporate IM-1 into RP-2 and IM-2 into RP-3 (there is a RP-1 subcategory already). Remove the Improvements (IM) Category.
20	SSA	27	Table 2	Appendix A	Information on Table 2 is incomplete. Maintenance -MA is not listed under the "Protect function" and Response Planning -RP is not listed under the "Respond” function.	Suggested Improvement: List Maintenance -MA under the "Protect function" and Response Planning - RP under the "Respond function on Table 2.
21	SSA	42	699-701	Appendix E	Framework: A risk-based approach to reduce cybersecurity risk composed of three parts: the Framework Core, the Framework Implementation Tiers, and the Framework Profile. Also known as the "Cybersecurity Framework."	Suggested Improvement: Remove: “Also known as the “Cybersecurity Framework" and call it Cybersecurity Framework.