#	Organization	Commentor	Type	Page #	Line #	Section	Comment (Include rationale for comment)	Suggested change
2	NA	Charles Hunt		1	74 to 76	1	While it is entirely appropriate that the Cybersecurity Framework (CF) be voluntary as required by the Executive Order, the CF should clearly articulate control objectives that should be implemented across all CI organizations. Various CI sectors have specialized needs, however, the core control objectives would help to establish the level of controls necessary to begin the effective management of cybersecurity risks. These core control objectives would assist Senior Management and Boards of Directors in understanding threats and risks facing the organization, provide clear guidance on appropriate levels of risk tolerance, and help to identify the highest priorities for remediation. The core control objectives should be stated in terms of verifiable outcomes and not specific implementation methods consistent with Appendices A and B.	Due to the increasing pressures from external threats, organizations responsible for critical infrastructure need to have a consistent baseline of cybersecurity outcomes and iterative approach to identifying, assessing, and managing cybersecurity threats and risks.
1	NA	Charles Hunt		i	11 to 12	Note To Reviewer	As written, any company that voluntarily adopts the Framework is allowed extraordinary discretion in the implementation of the standards and controls found in Appendices A and B. This discretion undermines the effectiveness of the Framework.	Generally, there need to be a series of changes to ensure that the Framework meets this objective - these are addressed in other comments and suggested changes
3	NA	Charles Hunt		1	82 to 83	1	Need to be clear that the Framework expresses common baseline outcomes	Because each organization's risk is unique, along with its use of IT and ICS, the tools and methods used to achieve the outcomes described by the Framework will vary.
4	NA	Charles Hunt		1	85 to 87	1	Many sources treat Cybersecurity as part of operational risk	key objective of the Framework is to encourage organizations to consider cybersecurity risk as a critical component of operational risk with a priority similar to financial, safety, and other aspects of operational risk while factoring in larger systemic risks inherent to critical infrastructure.

5	NA	Charles Hunt		1	88 to 91	1	Need to be clear that the Framework expresses common baseline outcomes and improve clarity	The Framework relies on existing standards, guidance, and best practices to achieve baseline outcomes to help protect critical infrastructure and that can assist organizations in managing their cybersecurity risk. By relying on those practices developed, managed, and updated by industry, the tools and methods available to achieve the baseline outcomes will evolve with technological advances and business requirements.
6	NA	Charles Hunt		1 to 2	95 to 104	1	Need to be clear that the Framework expresses common baseline outcomes and improve clarity	Building off those standards, guidelines, and practices, the Framework provides a common language and mechanism for organizations to: 1) describe their current cybersecurity posture relative to the baseline outcomes from the Framework; 2) describe their target state for cybersecurity; 3) identify and prioritize opportunities for improvement within the context of risk management; 4) assess progress toward baseline outcomes and the organization's target state; 5) foster communications among internal and external stakeholders. The Framework complements, and does not replace, an organization’s existing business or cybersecurity risk management process and cybersecurity program. Rather, the organization can use its current processes and leverage the Framework to identify opportunities to improve the organization’s management of cybersecurity risk. Alternatively, an organization without an existing cybersecurity program can use the Framework as a reference to establish one.
7	NA	Charles Hunt		3	145 to 148	1.1	A profile has to be assessed in context to something - by adding that the baseline objectives from the Framework are the basis, creating the profile is simplified and comparison between organizations becomes meaningful	Profiles are also used to identify opportunities for improving cybersecurity by comparing a “Current” Profile relative to the baseline outcomes from the Framework with a “Target” Profile. The Profile can then be used to support prioritization and measurement of progress toward the Framework baseline outcomes and the Target Profile, while factoring in other business needs including cost-effectiveness and innovation.

8	NA	Charles Hunt		3	164 to 168	1.2	Optimization is attractive conceptually but is at best only achievable in short time spans in which the relevant variables are nearly constant. the change helps to establish more reasonable expectations and will help to avoid low value added activities. Changes to the term common language will allow organizations to move forward without having to wait for / implement a standard method of assessing and quantifying risk - this will simplify adoption and implementation of the Framework by allowing each organization to build on their existing risk management processes.	With an understanding of risk tolerance and their Current and Target Profiles, organizations can prioritize systems that require attention. This will enable organizations to make informed decisions about cybersecurity expenditures. Furthermore, the implementation of risk management programs offers organizations the ability to quantify and communicate changes to organizational cybersecurity. Consistently quantified risk is the basis of common terminology for the organization that can facilitate communications to internal and external stakeholders.
9	NA	Charles Hunt		3	170 to 172	1.2	improve clarity and speed implementation	The Framework supports consistent risk assessment to help an organization select target states for cybersecurity activities that reflect baseline outcomes from the Framework and the organization's risk tolerance.
10	NA	Charles Hunt		5	200 to 205	2.0	Clarifies how the Framework can be used and how organizations and Sectors can build on the Framework. This will simplify implementation, help ensure consistent interpretation, and promote meaningful comparison and communication.	The Framework provides a set of baseline outcomes that creates a common language for expressing, understanding, and managing cybersecurity risk, both internally and externally. The Framework can be used to help identify and prioritize actions for reducing cybersecurity risk and is a tool for aligning policy, business, and technological approaches to managing that risk. Different types of entities, including sectors, organizations, and associations, can use the Framework as a starting point documenting extensions that reflect threats or risks that are sector (etc.) specific.
11	NA	Charles Hunt		6	227 to 228	2.1	Clarifies the definition of Subcategories, how the Framework can be used, and how organizations and Sectors can build on the Framework. This will simplify implementation, help ensure consistent interpretation, and promote meaningful comparison and communication.	Subcategories further subdivide a Category into high-level baseline outcomes that should be in place across all Critical Infrastructure Sectors. The subcategories contained in the framework are not intended to be a comprehensive set of practices to support a category for a given Sector or Organization. Sectors and Organizations are expected to develop extensions as necessary.
12	NA	Charles Hunt		8	299	2.2	A profile has to be assessed in context to something - by adding that the baseline objectives from the Framework are the basis, creating the profile is simplified and comparison between organizations becomes meaningful	Revise the diagram to reflect assessment of Current capabilities vs. Core Outcomes.

13	NA	Charles Hunt		11	414 to 416	3.2	Clarify the instructions for the creation of the current profile, includes support for organizational and Sector extensions to the framework while allowing flexibility in the tools and methods used. This change will simplify implementation and reduce costs to organizations opting to implement the Framework	Step 2: Create a Current Profile. Beginning with the Subcategories specified in the Framework Core, the organization develops a Current Profile that reflects its understanding of its current cybersecurity outcomes in relation to the baseline outcomes expressed in the Framework and any organization and Sector extensions based on its implementation of each Subcategory.
14	NA	Charles Hunt		13 (and 15)	446	Appendix A	Appendix A does not include adequate guidance (baseline outcomes) for outsourced functions, systems, use of cloud technologies (e.g. IAAS, SAAS, etc.). the addition will apply the framework requirements to third party service providers without having to duplicate and harmonize a new set of Framework subcategories. This makes the framework easier to understand and makes it clear to all vendors that provide services to Critical Infrastructure organizations what cybersecurity outcomes they need to support.	Add a new Subcategory to the Governance Category ID.GV-'5' Require Vendors (i.e. Third Party Service Providers) that provide material support for Critical Infrastructure to demonstrate that their cybersecurity outcomes support the baseline outcomes expressed in the Framework and any organization and Sector extensions that apply.