#	Organization	Commentor	Type	Page #	Line #	Section	Comment (Include rationale for comment)	Suggested change
1	Wohnig | Chaman | Associates	Ernest W. Wohnig III				Proposed Cover Letter	We have seen recent cases of prior NIST guidance (not standards) documents for industry being utilized by local regulators at the advise of audit service vendors for use as standards-like compliance measures when auditing utilities. Since this is not and should not be the intend of NIST guidance documents directed at assisting in the identification and assessment of an organization's cybersecurity risk, a cover letter directly addressing the issue to the critical stakeholders will prevent any confusion on the issue. I assume NIST does not intend for this to become a default regulatory auditing standard. Additionally, a cover letter (or to a slightly lesser degree inclusion of a section in the introduction) would be most directly viewed by senior regulators.	Inclusion of a cover letter to convey 'commanders intent' regarding the purpose and intended purpose of the framework. This would be include separate paragraphs that address industry senior leadership, the vendor services community, responsible national agencies, and most importantly local and state regulators. The letter should briefly layout the scope and intent (and in the case of regulators non-intended; i.e. audit purposes) of the Framework. At the least, a separate section in the introduction should address this issue directly to the above mentioned stakeholders. Since some of this information is included in the existing introduction this would help clarify and highlight it for these stakeholders.
2	Wohnig | Chaman | Associates	Ernest W. Wohnig III				Proposed Exec Summary	As one of the intents of the Framework is to increase the level of integration of cybersecurity risk into the larger business risk activity and to ensure support of business objectives, the framework will need exposure to those risk stakeholders. Those influential stakeholders are generally in senior management and regulatory positions. Therefore a one page Executive Summary that they can quickly review or that the cybersecurity professional can quickly turn into a memo, short presentation, or 10 min discussion with them would produce a large impact on utilization and awareness with minimal effort. This could also be expanded slightly to address most of the issues identified in our #1 comment above.	Include a one page Executive Summary to the Framework for non-cybersecurity focused senior leadership within the CIP organization and regulators.

3	Wohnig | Chaman | Associates	Ernest W. Wohnig III				3.2	It is important that the document articulates the organization may have different 'segments/enclaves' of the business. Further the included text should encompass the ideas that different enclaves/segments may have different risk tolerance and profiles associated with different business functions and environments. These needs to be taken into account when determining the overall posture and in some cases were completely isolated enclaves/segments exist the organization may have more than one cybersecurity posture (or sub postures).	Include a couple of paragraphs or a subsequent sub section that provides clear, specific language addressing the concept of Business Operations (i.e. ICS) vs. Enterprise sides of the organization.
4	Wohnig | Chaman | Associates	Ernest W. Wohnig III				Appendix C	This sub section should address individual industries' cybersecurity challenges/concerns via augmentation of the current Framework document or development of a family of documents delineated by individual industries.	Include a sub section identifying the need to address sector specific (i.e. utilities, oil & gas, water, manufacturing, etc.) cyber security risk issues in the future.