#	Organization	Commenter	Type	Page #	Line #	Section	Comment (Include rationale for comment)	Suggested change
1	American Chemistry Council	ChemITC	G			All	ACC supports the NIST Cybersecurity Framework and believes it provides a reasonable approach for members of the Chemical Sector and other critical infrastructure sectors to understand, communicate, assess and address cybersecurity risks within their organization. The Framework provides a structured process for managing cybersecurity risk that is flexible and scalable; which can be applied across a wide array of organizations, both large and small.	
2	American Chemistry Council	ChemITC	G			All	Given the ever evolving, dynamic nature of the cybersecurity threat, the Framework appropriately, does not seek to prescribe specific security mitigation measures and relies on the innovative process of the private sector to identify and address the threats and vulnerabilities applicable to their unique operating environment. However, the Framework does provide a clearinghouse of existing industry standards and best practices that can be used to help an organization build their own program.	

3	American Chemistry Council	ChemITC	G			All	The NIST framework should encour	Encourage the telecommunications providers, IT infrastructure (operating systems, databases), and solutions providers to make networks more secure by design.
4	American Chemistry Council	ChemITC	G			All	There should be clearer recognition for companies that adopt the framework. What rewards are available to companies that adopt the framework?	
5	American Chemistry Council	ChemITC	G			All	The framework primarily focuses on traditional IT security. More substance maybe needed in the framework on process control security.	A coordinated plan for both traditional IT security concerns and process or automation control cyber security should be included.
6	American Chemistry Council	ChemITC	G			Appendix B	Appendix B covers privacy and civil liberty issues and is a positive addition to the Framework. However, the privacy and civil liberties additions should be integrated into the Framework Core since implementation should be as important as any of the other controls, practices and standards.	Integrate privacy and civil liberty issues into the body of the framework.

7	American Chemistry Council	ChemITC	G			Section 2.2	The Framework Profile in section 2.2 should be expanded to include some practical examples of Categories and Subcategories and how companies can use them to drive the direction and maturity of their security program. While many large companies may relate to the concept of a Current Profile and a Target Profile and concepts of Categories and Subcategories, many smaller companies and users who are new to the cyber security world will not really understand the Profile approach in its current definition in the Framework.	Revise Section 2.2

8	American Chemistry Council	ChemITC	G			Section 2.4	The Framework describes a set of "Implementation Tiers" in general terms, but fails to define how an organization would actually determine what tier it is in for each of the five "Functions". ACC recommends that NIST consider documenting the minimum Categories/Subcategories that must be met for each implementation Tier or alternatively, at least rank the Categories/Subcategories by importance. The Framework does not document how a company can calculate its overall Implementation Tier. The Framework should provide guidance on how one can go about developing criteria to implement each Tier for the five Functions.	Revise Section 2.4
9	American Chemistry Council	ChemITC	G			All	The relationship of an organization's adoption of the framework to the framework tiers is unclear	Connect an organization's risk profile to the tier structure.

10	American Chemistry Council	ChemITC	G			All	The framework says "The Informative References presented in the Framework Core are not exhaustive but are example sets, and organizations are free to implement other standards, guidelines, and practices." However, the Framework Core is not designed to allow practitioners to easily do this. ACC recommends that the Framework Core add additional columns to (1) allow users to document the standards, guidelines and practices they will implement to meet the objectives for each Category/Sub-Category and (2) allow users to document any gaps they identify.	Revise.
11	American Chemistry Council	ChemITC	G			All	It should be stated that organizations have the flexibility to determine the scope of the framework's implementation - such as across critical assets, facilities or business units.	Clarify implementation scope.
12	American Chemistry Council	ChemITC		i	15	Note to Reviewers	The framework does not provide tools for senior executives and boards of directors to understand risks and mitigations at the appropriate level of detail	Develop solutions to enable effective communication to senior executives and boards of directors to understand risks and mitigations at the appropriate level of detail
13	American Chemistry Council	ChemITC		1	77-83	1.0 Framework Introduction	The term "critical function" should be added to the glossary, and better explained.	Add "Critical Function" to the glossary.

14	American Chemistry Council	ChemITC				1.0 Framework Introduction	There is an opportunity to connect the framework to Sector Specific Plans and the critical functions described. Also, this paragraph introduces the idea of cross-sector interdependencies, which are not addressed in the framework practices.	Identify critical practices as described within sector specific plans, where possible, use those functions to build risk evaluation criteria. Add cross-sector interdependency risk management practices to the framework.
15	American Chemistry Council	ChemITC		1	83	1.0 Framework Introduction	The term " implementation of the Framework" is added and should be in the glossary	Define what is meant by "Implementation of the Framework" in the glossary
16	American Chemistry Council	ChemITC		1	84-87	1.0 Framework Introduction	A key objective of the framework should be to manage critical infrastructure risk, not all cyber security risk. There are some cyber security risks that should remain outside of the scope of the framework (risk to information systems that relate to profitability, for example). While those risks are important for the business, they should remain outside the realm of a critical infrastructure protection framework.	Focus on critical infrastructure risk and only business risks that are directly related to the critical infrastructure services provided that are so significant that failure can cause corporate failure.
17	American Chemistry Council	ChemITC		1	84-87	1.0 Framework Introduction	The framework does not identify outcomes that should be achieved.	Identify desired outcomes of framework implementation

18	American Chemistry Council	ChemITC		1	95-99	1.0 Framework Introduction	The framework does not provide organizations a mechanism to describe their cybersecurity posture, unless the various tiers are intended to be that description, however, based on lines 82-83, each organization will implement the framework differently, so there will be no common description of posture. Similarly, if each organization will implement the framework differently, target state definition will vary by organization needs. The framework lacks useful scoping guidance for implementation, so organizations are likely to be challenged to establish targets and to prioritize improvement. Beyond the coarse "tier 1/Tier 2 etc. designations, it is unclear how the framework fosters communication among internal and external stakeholders.	Reevaluate these stated conditions, and explicitly drive the framework to achieve them. Currently, they are not supported by the content in the framework.
19	American Chemistry Council	ChemITC		2	140-149	1.1 Overview of the Framework	The concept of the framework profile may be useful, but there are no mechanisms to enable an organization to determine their current "as-is" profile, or to determine their future-state profile. Also, it would likely be useful if the future state profile were connected to their potential impact to their critical functions.	Develop a mechanism to identify the current profile of an organization, as well as assistance to assist organizations to determine what their future state profile should be, considering risk to critical infrastructure or the nation.

20	American Chemistry Council	ChemITC		3	160-162	1.2 Risk Management and the Cybersecurity Framework	The concept that CIKR need to understand their risks is more important than how the authors address it here. The impacts that CIKR are subject to are what defines critical infrastructure. That being said, not all impacts are of national concern. An important point is that some (not all) impacts from cybersecurity risk to CIKR is what the nation has an interest in mitigating. Thus, the government should have a role in assisting CIKR in identifying (and mitigating) these select impacts,	Recognize that not all risks are equivalent, and thus not all impacts are the focus of risk management activities. Furthermore, the defining characteristic of critical infrastructure is that they may be exposed to risks that result in impacts that are of national significance. The government should have a role in assisting in the identification, measurement and mitigation of these risks. Else, the scope of this framework is too broad to address the core problem of Critical infrastructure cybersecurity.
21	American Chemistry Council	ChemITC		9		2.1	Encourage standards development organizations to develop maps linking their standards to the framework.	Add roadmap encouragement.