#	Organization Name	Submitted By	Type*	Section / Page / Req #	Comment (Include rationale for comment)	Suggested change
1	DoD (MITRE)	Julie Snyder	Substantive	Main CSF Document: Executive Summary / pg. 1 / Lines 113-115 (mark-up version)	Recommend referencing mission and business requirements collectively. "Mission" is a more intuitive term for federal agencies, and is also applicable to private sector organizations (e.g., mission statements that are part of organizational strategies). Also, some people see a distinction between mission and business requirements and functions, and this shows that when viewed separately both views are important. Change is consistent with other areas of the document where there is a reference to "business/mission."	Recommend editing this sentence as follows (see red text): "Through use of Profiles, the Framework will help an organization to align and prioritize its cybersecurity activities with its business/mission requirements, risk tolerances, and resources."
2	DoD (MITRE)	Julie Snyder	Substantive	Main CSF Document: Executive Summary / pg. 2 / Lines 130-132 (mark-up version)	Recommend mentioning other sectors and communities for consistency with the new sentence at line 123-124. While critical infrastructure is likely to be the primary focus for international cooperation for quite some time, there's no reason this framework's use international cannot also be more broadly applied as it can be in the U.S.	Recommend editing this sentence as follows (see red text): "Moreover, because it references globally recognized standards for cybersecurity, the Framework can serve as a model for international cooperation on strengthening ~~critical infrastructure~~ cybersecurity in critical infrastructure as well as other sectors and communities."
3	DoD (MITRE)	Christina Sames	General	Main CSF Document: Executive Summary (clean version)	Include a paragraph on how the Cybersecurity Framework can be used to work with other frameworks (such as the RMF) by organizations in order to address cybersecurity risk management from strategic and tactical perspectives within an organization, from your most senior individuals to your "boots on the ground" employees, noting that the Framework is intended to work with other frameworks or processes within organizations. This type of paragraph is included on page 4 of Section 1.0 but it is a bit hidden, and the message in this paragraph is important enough for it to be in the Executive Summary and noted/called out in the main body of the document itself.	
4	DoD (MITRE)	Christina Sames	Editorial	Main CSF Document: Section 1.0 / pg. 3 / paragraph 1 / line 134 (clean version)	Remove mention of "controls" in this paragraph and replace with "safeguards" or another similar type word ("engineering"?). This way, the focus is on the activities that would achieve the goal of managing risk versus identifying the controls (e.g., 800-53 security controls) that people would be looking to implement for compliance, especially if private industry is to be a user of this Framework and Roadmap.	Change to read, "…including information security measures and safeguards that may be…"
5	DoD (MITRE)	Christina Sames	Editorial	Main CSF Document: Section 1.0 / pg. 4 / lines 168-170 (clean version)	Include that integrating privacy and cybersecurity can also create or enable standardized protecting of information. Creating standardized protections can also increase customer confidence and supports standardized sharing of information.	Change last sentence to read, "…enabling more standardized protecting and sharing of information,".
6	DoD (MITRE)	Julie Snyder	Substantive	Main CSF Document: Section 1.0 / pg. 3-4 / Lines 187-192 (mark-up version)	Recommend more directly acknowledging federal agency use. The terminology used broadly covers other areas of critical infrastructure, but does not lend as easily to federal agencies seeing themselves in the framework beyond the individuals that have a role in sector coordination (an externally facing role vs. internal use of the framework). Recommending appending this thought as its own sentence to avoid any concerns my non-federal entities that they would be subject to concerns that may not apply to them.	Recommend editing this sentence as follows (see red text): "For example, as technology and the data it produces and processes is increasingly used to deliver critical services and support business/mission decisions, the potential impacts of a cybersecurity incident on an organization, the health and safety of individuals, the environment, communities, and the broader economy and society should be considered. Federal agencies should consider these potential impacts as well as those to the functioning of the executive branch."
7	DoD (MITRE)	Julie Snyder	Substantive	Main CSF Document: Section 1.1 / pg. 5 / Lines 241-242 (mark-up version)	"Mission" is a more intuitive term for federal agencies, and is also applicable to private sector organizations (e.g., mission statements that are part of organizational strategies). Also, some people see a distinction between mission and business requirements and functions, and this shows that when viewed separately both views are important. Change is consistent with other areas of the document where there is a reference to "business/mission."	Recommend editing this sentence as follows (see red text): "Each Framework component reinforces the connection between business/mission drivers and cybersecurity activities."

8	DoD (MITRE)	Julie Snyder	Substantive	Main CSF Document: Section 1.1 / pg. 5 / Lines 269-272 (mark-up version)	"Mission" is a more intuitive term for federal agencies, and is also applicable to private sector organizations (e.g., mission statements that are part of organizational strategies). Also, some people see a distinction between mission and business requirements and functions, and this shows that when viewed separately both views are important. Change is consistent with other areas of the document where there is a reference to "business/mission." Referencing mission here also helps when discussion Mission Objectives as they support Profile development. Consider making this change globally throughout the document where business requirements, needs, objectives, etc., are mentioned.	Recommend editing this sentence as follows (see red text): "To develop a Profile, an organization can review all of the Categories and Subcategories and, based on business/mission drivers and a risk assessment, determine which are most important; it can add Categories and Subcategories as needed to address the organization's risks."
9	DoD (MITRE)	Christina Sames	General	Main CSF Document: Section 2.2 / pg. 10 / lines 383-386	Consider including that risk management process at Tier 1 may be compliance focused. Organizations may think they have a risk management process in place but it actually may be more compliance focused than risk management focused. It may be useful to address the compliance aspect in all Tiers in the "Risk Management Process" bullet, since compliance still is part of what an organization has to do regarding demonstrating how well it meets certain regulations/laws/federal requirements (ID.GV-3), but the ability to manage/demonstrate compliance while executing risk management is necessary, and not have compliance be considered the risk management process (this also ties in to the statement on lines 775-776 about artificial indicators of current state and progress in improving cybersecurity risk management). Additionally, it may also be beneficial to address the level of rigor applied by the organization within the various Tiers - ideally, as the organization has a better risk management process in place, not all systems or environments will be treated the same - there will be a heterogenous application in risk management versus a homogenous one.	
10	DoD (MITRE)	Christina Sames	General	Main CSF Document: Table 2 ID.GV-1 / pg. 26 (clean version)	The subcategory here should also address the communication of established policy. Policy is of no use if it is not communicated (successfully) across an organization, to all tiers of employees/implementers who are to use it, so there is an awareness of what the policy, procedures, and processes are that should be in place and what should be applied.	
11	DoD (MITRE)	Julie Snyder	Admnistrative	Main CSF Document: Appendix A	Recommend pulling the Informative Reference out of the main Cybersecurity Framework document and housing them as a separate resource. While it is convenient to include the Informative References as part of the Framework Core, the references need to be easier to update more frequently, and housing them in a single location would be most useful to the user community. For example, NIST SP 800-53, Rev 5 is expected in 2018. Based on the substantive changes in the public drafts of Rev 5, there may be more than administrative changes to the Cybersecurity Framework's Informative References for Rev 4. Additionally, for federal agencies and contractors, references to NIST SP 800-171 would be useful to see along with the full list of Informative References, instead of in a separate document on the SP 800-171 document posting.	Prioritize some of the actions for Roadmap item 4.11 that are "quick wins" to begin separating the Informative References from the main CSF document.
12	DoD (MITRE)	Julie Snyder	Substantive	Roadmap: Section 4.5 / pg. 9	The second paragraph, which begins immediately following the bulleted list of federal requirements, does not seem to fit this section as written. It reads as a justification for including NIST SP 800-53 controls as an Informative Reference generally, which was more important when writing v1.0. Recommend reframing the paragraph to discuss how the inclusion of SP 800-53 controls will aid federal agencies in "hitting the ground running" with the framework. Also recommend acknowledging plans for incorporating any relevant changes with the forthcoming updates coming with SP 800-53 Rev 5. The 800-53 Rev 5 changes will be of particular interest to federal agencies, and non-federal organizations that use or are considering using this standard.	For example, consider reframing the paragraph to say something like: "Since federal standards and guidelines were cited by non-federal participants as useful in managing cybersecurity risk, the Framework already includes controls from NIST SP 800-53, Revision 4, the current version in use at the time of publication for v1.0 and v1.1 draft 2 of the Framework, as Informative References. This mapping provides federal agencies and other organizations that use SP 800-53 a starting point for determining how their current cybersecurity practices relate to Subcategories in the Framework Core. At the time of publication, NIST is in the process of updating SP 800-53, with Revision 5 planned for 2018." Considering including a footnote to the information published on Rev 5 as well as adding or referencing any existing NIST messaging regarding Rev 5 and the Cybersecurity Framework (e.g., greater alignment between CSF and 800-53 controls). Also reference in the bulleted list of anticipated future activities.

13	DoD (MITRE)	Julie Snyder	Editorial	Roadmap: Section 4.5 / pgs. 9-10	The order of the paragraphs that discuss NISTIR 8170 and NIST SP 800-37 - Revision 2 are inconsistent with the chronology of development and flow of the section as it moves on to discuss updates to other SPs.	Recommend swapping the order of the paragraphs that discuss NISTIR 8170 and NIS SP 800-37 - Revision 2.