Page #	Line #	Section	Existing Content	Recommended Change	Comment	Contact Info (if add'l info is requested)
2	97	1. Introduction	The NIST Cybersecurity Framework (Framework or CSF) describes…	The NIST Cybersecurity Framework (CSF), referred to in this document as The Framework, describes…	Recommend cleaning up additional descriptors to show that "The Framework" is how it is referred to in the document itself (I don't think it would be referred to as simply "The Framework" outside of this document due to lack of context)	Michael Hankins (michael.j.hankins@lmco.com) Lockheed Martin
2	98	1. Introduction	The voluntary Framework…	The Framework…	Lines 89-90 specify that CSF is adopted voluntarily AND through governmental policies and mandates, so it shouldn't be referred to as a purely voluntary document	Michael Hankins (michael.j.hankins@lmco.com) Lockheed Martin
6	234	2.1 Functions, Categories, and Subcategories	To form and maintain a culture that addresses dynamic cybersecurity risk, the Functions should be addressed concurrently	Recommend adding wording that takes into account initial application of the CSF vs system sustainment.	I agree that actions supporting all of the Functions should happen continuously, but when a system is first establishing its security posture, things need to be linear. For example, assets must first be identified/understood to know what to protect, the actions during the Protect Function enable detections/response/recovery, detections must occur before a response, etc. After a system has a mature CSF implementation in place, then yes, the Functions should be addressed concurently.	Michael Hankins (michael.j.hankins@lmco.com) Lockheed Martin
8	277	3. Using the Framework	With an understanding of stakeholder expectations and risk appetite and tolerance	With an understanding of stakeholder expectations, risk appetite, and tolerance	Recommend changing to a list rather than separating with multiple ands	Michael Hankins (michael.j.hankins@lmco.com) Lockheed Martin
13	453	Fig. 5. Cybersecurity Framework Tiers	Graphic has "For Risk Governance", "For Risk Management", and "For Third-Party Risks" layered over it	Can the overlayed "For" terms be relocated or shown in a different way that better shows the intent? I believe this graphic is trying to say that those are all risk areas that the tiered structure applies to, but there may be a better way to visually show that.		Michael Hankins (michael.j.hankins@lmco.com) Lockheed Martin
14	462	3.3. Using Framework Tiers to Characterize Cybersecurity Risk Management Outcomes	Progression to higher Tiers is encouraged when risks or mandates are greater or when a cost-benefit analysis indicates a feasible and cost-effective reduction of cybersecurity risks.	Progression to higher Tiers is encouraged depending on system criticality, when risks or mandates are greater, or when a cost-benefit analysis indicates a feasible and cost-effective reduction of cybersecurity risks.		Michael Hankins (michael.j.hankins@lmco.com) Lockheed Martin
15	498	Fig. 6. Using the Cybersecurity Framework to improve communication	Consider removing the "National" part of the graphic.	I don't quite understand how the "National" box ties in to the graphic. The other portions of the graphic make sense from a business communicaitons perspective, but the National part is outside the scope of many businesses.		Michael Hankins (michael.j.hankins@lmco.com) Lockheed Martin