#	Organization	Commentor	Type	Page #	Line #	Section	Comment (Include rationale for comment)	Suggested change
	NCOIC	JDB	Technical	1	86	1.0	Expand the text to emphasize more than just managing cybersecurity risk.	Replace lines 84-86 with: "This Framework, developed through collaboration of public and private sector subject matter experts, works to provide guidance to organizations to defend against and mitigate cybersecurity risk. A key objective of the Framework is to assist organizations with implementing best practices to create a defense in depth strategy against cyber attacks and to protect critical infrastructure and address larger systemic risks. Organizations must prioritize cybersecurity in the same manner as financial security, operational risk mitigation and life safety to ensure overall organizational health and stability."
	NCOIC	EB/WR	Technical	1	99	1.0	The Cybersecurity Framework should acknowledge the cross-domain (cross-sector) interoperability needs in today's operating environments, and the additional risks this may entail. Having a common cybersecurity framework facilitates secure cross-domain interoperability.	Add a paragraph after line 99: "An additional benefit of using a common cybersecurity framework is that it helps manage cross-sector risks, thus the facilitating secure cross-sector interoperability which is becoming more important in today's operating environments."
	NCOIC	Butler	Technical	3	161	1.2	Use of word "risk".	Replace "an adverse event" in place of "a risk event".

	NCOIC	WJP	Technical	5	207	2.1	The framework should stress managing cybersecurity across enterprises.	Replace sentence at line 207 with: "The Framework Core provides a holistic view of references to cybersecurity activities and Informative References. The Framework Core is not a checklist of activities to perform; it presents key cybersecurity outcomes that are aligned with activities known to manage cybersecurity risk across an enterprise."
	NCOIC	WJP	Technical	6	246	2.1	The risk assessment needs to look at both immediate risk from known malware types as well as projection of potential new forms of malware that could be encountered in the future but have not been actually fielded yet.	Change the text in line 246 from "Risk Assessment, and Risk Management Strategy" to Risk Assessment, and Risk Management Strategies for both immediate risk from known malware types to potential future risk from projected possible new forms of malware that have not yet been fielded but are technically plausible".
	NCOIC	BRC	Technical	8	308	2.3	Cybersecurity risks are often well understood by the IT employees, but not well understood by the executives who make investment decisions. Especially in cases where IT is outsourced, communication barriers and insufficient information flow are detrimental to senior executive level understanding of the real cybersecurity risks. Summary level risk reports may not be sufficient.	Add text to section 2.3 along the following lines: "The risk reports provided to the senior executives must be sufficiently detailed with regard to the cybersecurity risks such that the executives can make informed decisions. Figure 3, which is notional, does not preclude direct communication between the senior executive level and implementation/operations level, which is often times beneficial".
	NCOIC	Butler	Technical	11	393	3.0	While "programs" are understood to include associated systems, this change makes it explicit.	Append "and associated systems" to the end of the sentence, line 393. Becomes "… for improving an existing program and associated systems".

	NCOIC	WJP	Technical	12	422	3.2	Recommend that industries and sectors develop a best practice model template to allow organizations developing their own template to sanity check their target profile against one based on their sectors lessons learned based model to allow for more accurate gap analysis.	Recommend adding following text to "Step 4", on line 424. "Use a sector or industry baseline Target Profile as a starting point if one exists and is appropriate."
	NCOIC	MKB	Technical	12	441	3.3	The supply chain can be an important location for cybersecurity risk, and should be explicitly mentioned.	Change text to read: "An organization may utilize a Target Profile to express requirements to an external service provider (e.g., a cloud provider) or to a supply chain partner with whom they exchange information."
	NCOIC	MKB	Technical	13	463	Appendix A	For clarity.	Please add a note clarifying whether the Informative References shown in Table 1 are meant to apply to all profiles, or if are they just examples.