Comment No.	Section	Page	Line	Section Title	Comment Text	Recommendation
1	Note to Reviewers	iii	30	Note to Reviewers	Yes, the inclusion of supply management controls into the framework and the addition of the cyber-attack lifecycle and metrics to the roadmap are relevant.	
2	Note to Reviewers	iii	33	Note to Reviewers	Yes, where we use the NIST CSF 1.0 as a basis for cybersecurity risk management, we will need to update them to the new version. This activity is beneficial as it is an industry vetted process improvement. The approach used to update the framework, minimal changes to 1.0 sections, will simplify the update process.	
3	Executive Summary	1	106	Executive Summary	Include acknowledgement of existing standards, regulations, and other voluntary frameworks that contribute to the overall cybersecurity posture of an organization.	Add language "There are many ways to achieve security and organizations should not be limited in their approach. This Framework recognizes that there are existing standards and regulations, as well as other voluntary frameworks for organizations to use for cybersecurity risk management."
4	Executive Summary	2	127	Executive Summary	...to apply the principles and best practices of risk management to improving security and resilience.	...to apply the principles and best practices of risk management to improving cybersecurity and resilience of the Information Technology (IT) and Operational Technology (OT) infrastructure.
5	Executive Summary	2	141	Executive Summary	Include acknowledgement of the dynamic nature of cyber adversaries and that use of the Framework cannot be a silver bullet	Add language after ..."infrastructure.": "This Framework recognizes that innovation by cyber adversaries is dynamic, and defending against them requires organizations to react constantly. As a static document, the Framework cannot be expected to provide full protection from those adversaries."
6	Executive Summary	2	152	Executive Summary	What defines the term "best practices"? Is this based from other industries, an aggregation of a given industry collectively, or based on federal recommendations of securing our infrastructures?	
7	1.0	4	206	Framework Introduction	spelling error	suggest changing "support" to supports"
8	1.2	6	281	Risk Management and the Cybersecurity Framework	grammatical error	suggest changing "their" to "its" for consistency
9	2.0	10	354	Framework Core	These Functions are not intended to form a serial path, or lead to a static desired end state.	This comment implies that you can dive into any of the functions, however, the first function (Identify) then stats that Identify is foundational. It might be better to re-phrase that the functions are continuous and circular, versus concurrently.
10	2.2	10	411	Tier 2: Risk Informed	Change language	Replace "should" with "could" to indicate that although the Framework can be used as a tool to assist in resource prioritization for companies, the identification of "tiers" and their corresponding level of cybersecurity controls does not compel the allocation of resources in a particular manner. Resource prioritization among the objectives of an organization may differ from that outlined in the Framework for a variety of reasons beyond the scope of the Framework.
11	2.1	11	379, 381, 385, 387	Framework Core	Event or incident?	We still respond and recover from events, which may not rise to the level of incident.
15	2.2	11	389	Framework Implementation Tiers	The use of independent audit/assessment of risk should be explicitly included in the appropriate tier(s).	
16	2.2	11	409	Framework Implementation Tiers	addition of the work "necessarily" introduces ambiguity in how the Tiers should be interpreted.	Remove "necessarily"
18	2.2	12	461, 484, 519	Tier 4 Adaptive	Lines 461, 484, and 519: Remove references to "formally" and "formal" that characterize the organization's response to cyber supply chain risks. Depending on the nature of the risk identified, less formal responses could be appropriate. A requirement to "formally" respond could unnecessarily delay responses to risks or require additional paperwork and process without meaningful benefits to the substance of the response, such as if a supplier reports routine phishing attacks on its corporate network.	The descriptions of the tiers should call for responding in a manner commensurate with the risk, which could be more or less formal depending on the severity and urgency of the specific reported risk.
19	2.2	13	422	Framework Implementation Tiers	The tendency may be to over estimate capabilities and thus assume a higher Tier than warranted	Consider including examples of organizations in the Tiering section
20	2.2	13	437	Framework Implementation Tiers	dependencies and dependents	the terms "dependents" and "dependencies" are introduced as new terms and should defined in the glossary
21	2.2	13	455-457	Framework Implementation Tiers	need to clarify "but not both"	Suggest changing language to "Generally, the organization understands its role in the larger ecosystem with respect to **either** its own dependencies**,** or dependents**,** but not both.
22	2.3	15	521	Framework Profile	"Profile" as explained sounds synonymous with "Maturity"	
23	2.2	15	506	Framework Implementation Tiers	business/mission objectives	change to "organizational objectives" for consistency
24	2.2	15	514	Framework Implementation Tiers	threat and technology landscape evolves	Suggest changing to threat and technology **landscapes evolve**.

25	2.2	15	516	Framework Implementation Tiers	real-time or near real-time	This criterion feels aspirational, as it should be since it is the highest implementation tier. Given the present state of technology and relationships between suppliers and buyers, wherein buyers should, in theory, have the upper hand but, in reality, suppliers often are dictating agreement terms (for a variety of reasons). The need for supplier cooperation needs to be explicitly stated as an expectation.
26	3.0	18	570	How to Use the Framework	The framework also applies to earlier phases of the lifecycle.	Change "...life cycle phases of design, build/buy,…" to "...life cycle phases of plan, design, build/buy,…"
27	3.3	20	670	Communicating Cybersecurity Requirements with Stakeholders	"an organization can better manage"	suggest changing to "an organization may manage" for consistency and parallel structure.
28	3.3	20	674	Communicating Cybersecurity Requirements with Stakeholders	"a complex, globally distributed, and interconnected set of resources"	Suggest changing to "complex, globally distributed, and interconnected sets of resources" (remove "a" and change "set" to "sets")
29	3.3	20-21	673-718	Communicating Cybersecurity Requirements with Stakeholders	The inclusion of SCRM throughout the various sections of the CSF (instead of having its own section and implementation tiers) is an improvement, however it seems out of place, like it's been copied and pasted	Recommend moving to section 3.4 and changing title to "Cyber Supply Chain Risk Management"
30	3.3	21	683-685		This definition below of Supply Chain Risk Management from NIST.SP.800-161 April 2015 does not cover the threat actors which hack vendors with malicious intent to take data or interrupt business processes. It may be helpful to add a sentence to address this.	At a minimum, we could recommend that they amend the definition as follows: "…vulnerable due to inadequate cybersecurity controls, or poor manufacturing and development practices within the cyber supply chain."
31	3.4	23	722	Buying Decisions	"cyber SCRM (Section 3.3)"	Section 3.3 has a new title - Communicating Cybersecurity Requirements with Stakeholders
32	3.4	23	731	Buying Decisions	The CSF does not address remote access by vendors	Suggest adding language "The organization also recognizes that products and services may include periodic or persistent remote access by the product supplier and/or integration firms. This remote access should be periodically reviewed and assessed with a cybersecurity focus regarding who from the supplier or integrator is able to connect remotely and what are they able to access. Review of the cybersecurity controls of the supplier and/or integrator company are necessary to ensure compromise of their systems does not become an attack vector to the purchasing organization."
33	3.6	24-25	775-802	Methodology to Protect Privacy and Civil Liberties	seems out of place in the document	Align the privacy and civil liberties controls with the Framework Core instead of having a separate taxonomy
34	4.0	26		Self-Assessing Cybersecurity Risk with the Framework	The section does not seem to add much to the document and just restates the process and general commentary made earlier in the document.	Remove the section for conciseness or provide more detailed guidance (perhaps as an appendix).
35	4.0	26	803	Self-Assessing Cybersecurity Risk with the Framework	This section is an improvement from the previous metrics and measures section in draft 1, but should be edited for clarity and voice.	
36	4.0	26	841	Self-Assessing Cybersecurity Risk with the Framework		remove "lagging" and "leading," or add back in the definitions in the glossary that were proposed in draft 1 (which have been removed in draft 2)
37	4.0	26	842	Self-Assessing Cybersecurity Risk with the Framework	"cybersecurity risk may occur, and the impact it might have"	suggest changing "may occur" to "exists" … risks do not occur, they exist
38	Appendix A	29	N/A	ID.SC-2	Subcategory ID.SC-2: The subcategory presumes that purchasers will have the ability to perform a meaningful assessment of suppliers as part of a risk assessment process. However, many buyers will have limited, if any, visibility into some or all of their suppliers' risks, particularly for suppliers upstream of the purchaser's direct supplier. Therefore, the language should make clear that completing such assessments depend on and are limited by the available information.	For example, the phrase "using reasonably available information" could be added to the end of the sentence.
39	Appendix A	29	N/A	ID.SC-3	Subcategory ID-SC-3: The subcategory assumes that a contract will exist and that the buyer will have sufficient leverage to require that the contract include the necessary security terms. However, in many cases, goods presenting cybersecurity risk are purchased off-the-shelf without any means to require any supplier contract terms on security. In other cases, a purchaser may have limited or no leverage over its suppliers, particularly for legacy systems or for narrow industry segments with only one or a handful of potential suppliers.	The subcategory should account for these circumstances such as through the following changes: "Where contracts with suppliers and third-party partners are used for the delivery of products and services, the organization seeks contract terms requiring suppliers and third-party partners ~~are required by contract~~ to implement appropriate measures designed to meet the objectives of the Information Security program or Cyber Supply Chain Risk Management Plan."

40	Appendix A	29	N/A	ID.SC-4	Subcategory ID.SC-4: The subcategory assumes that a contract exists and that the buyer will have sufficient leverage to require that the contract include supplier security assessment provisions. That may not be possible if the products are off-the-shelf or if the purchaser lacks sufficient leverage to require vendor agreement to those provisions.	The subcategory should be modified as follows: "Where contracts with suppliers and third-party partners are used for the delivery of products and services, the organization seeks the ability to routinely assess suppliers and third-party partners ~~are routinely assessed~~ to confirm that they are meeting their contractual obligations. Reviews of audits, summaries of test results, or other equivalent evaluations of suppliers/providers are conducted."
41	Appendix A	30		Table 2	The updated category, subcategories, and information reference are a useful addition to the document.	Keep the updates.
42	Appendix A	30		Table 2	The CIS CSC controls have a version associated with the definitions. Also, each control is also comprised of practices and, where appropriate, referring to those specific practices instead of the entire control would be helpful.	Add CIS CSC control set version number. Specify specific control activities where appropriate.
43	Appendix A	30		ID.AM-5	What does "time" refer to?	
44	Appendix A	30		ID.AM-5	Consider personnel as an added resource	(e.g. personnel, hardware devices, data, time, and software)
45	a	30	N/A	ID.SC-5	Subcategory ID.SC-5: The subcategory assumes that suppliers will participate in response and recovery planning and testing, when that may not be possible due to supplier unwillingness.	The subcategory should be modified as follows: "Response and recovery planning and testing are conducted with suppliers and third-party providers where those suppliers and third-party providers are willing to participate in such activities."
46	Appendix A	34		ID.SC-2	The "Subcategory" language describing ID.SC-2 should be written in passive voice, if possible (I have proposed one option), in order to match the structure of the rest of the framework.	Suggest changing to "Suppliers and third-party partners of information systems, components, and services are identified, prioritized, and assessed using a cyber supply chain risk assessment process.
47	Appendix A	34		ID.SC-3	Use of "required" is too prescriptive	Suggest changing to "may consider contractually obligating the other party to implement…"
48	Appendix A	34		ID.SC-3	states that suppliers are "required by contract to implement appropriate measures designed to meet objectives of the Info Sec program or Cyber SC RM plan." However, 3.4 Buying Decisions on page 23 mentions on line 722 that "it may not be possible to impose a set of cybersecurity requirements on the supplier."	These statements seem contradictory and should perhaps be reworded?
49	Appendix A	34		ID.SC-3	Suggest update in language	Suppliers and third-party partners are required by contract to implement security measures, as appropriate or as required for the contracted services, designed to meet the objectives of the information Security program or Cyber Supply Chain Risk Management Plan.
50	Appendix A	35		ID.SC-4	Does this mean to be fully compliant an organization must conduct audits of suppliers?	
51	Appendix A	35		ID-SC-5	Does this mean to be fully compliant an organization must exercise with its suppliers?	
52	Appendix A	35		ID.SC-5	May prevent smaller companies from achieving the desired tier as worded.	Suggesting changing to "Suppliers and third-party partners verify each other's response and recovery plans."
53	Appendix A	35		ID.SC-4	Suggest update in language	Suppliers and third party partners are routinely assessed to confirm that they are meeting their contractual obligations. Reviews are conducted on audits, summaries of test results, or other equivalent evaluations of suppliers/service providers.
54	Appendix A	35		ID.SC-4	Who is conducting the audit? Is this a requirement for the client of the service provider to conduct the audit or just review the results of an audit?	If the latter is true, then this should read: Reviews are performed on the summary of audit results, summaries of test results, or other evaluations of suppliers/service providers.
55	Appendix A	35		PR.AC-1	Identities are not "issued"; however, credentials are.	Identities are verified, credentials are issued, access is managed, revoked, periodically recertified, and audited for authorized devices, users, and processes
56	Appendix A	35		PR.AC-2	Only mention of physical or personnel security. May consider additional areas relative to physical and personnel security.	Personnel Security Cross reference for NIST and ISO: NIST NIST 800-53r4: PS-1, PS-2, PS-3, PS-4, PS-5, PS-6,PS-7 and ISO: A.5.1.1, A.5.1.2, A.6.1.1, A.12.1.1, A.18.1.1, A.18.2.2. A.6.1.1*, A.7.2.1*
57	Appendix A	36		PR.AC-6	"Identities are proofed and bound to credentials, and asserted in interactions when appropriate" - This wording is not clear.	Suggest changing to "Identities are verified, with a one-to-one relationship to credentials, and are provided in interactions where it is appropriate to require proof of identity."
58	Appendix A	36		PR.AC-6	What does "asserted in interactions" mean?	Clarification needed.
59	Appendix A	37		PR.AT-2	"Privileged users…"	Suggest to update text to "Privileged Users" to match defined term in glossary.
60	Appendix A	37		PR.AT-3, 4, 5	Need to identify whose roles and responsibilities need to be understood. It doesn't do much good if the user understands everyone else's role and responsibilities but not their own.	suggest to update each line to include "their roles and responsibilities"
61	Appendix A	39		PR.DS-8	"Integrity checking mechanisms are used to verify hardware integrity" is too prescriptive	Suggest changing to "Hardware integrity validation is considered through configuration or through a checking mechanism"
62	Appendix A	41		RS.CO-2	Event or incident?	
65	Appendix A	43		PR.PT-5	I'm not quite sure how this fits in the "Protective Technology" section, as currently worded. Not sure where else it would belong, though. Perhaps it would help to somehow reference there being some 'technology' involved?	Maybe add language at the start to say "Failsafe protections exist that enable systems to operate in pre-defined functional states …." (in which case the "failsafe protections" would represent the "Protective Technology" in question).
66	Appendix A	48		RS.RP-1	Event or incident?	
67	Appendix A	50		RC.RP-1	Event or incident?	
68	Appendix B	53		Glossary	Previously used terms such as "dependents" and "dependencies" should be defined	

69	Appendix B	53		Glossary	If "lagging measurements" and "leading measurements" are going to be continued to be used, they should be defined	
70	Appendix B	53		Glossary	Define "organizational asset"	Suggested definition "All assets, human and non-human, that an organization has available to fulfill its mission, objectives, and goals."
71	Appendix B	53		Glossary	Define "operational technology"	Suggested definition "The collection of systems, control and instrumentation equipment, and networks specifically designed to maintain industrial-based operations. OT provides a supporting role for managing computing resources for ICS."
72	Appendix B	53		Glossary	Define "risk tolerance" As defined in NIST Special Publication 800-39: http://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-39.pdf	Suggested definition "Risk tolerance is the level of risk that organizations are willing to accept in pursuit of strategic goals and objectives."
73	Appendix B	55		Glossary	Need to further define what constitutes a “supplier,” lots of activities can be bundled into the term. Is the intent primarily critical services (risk based) or everything including mundane business services?	
74	Appendix C	56		Acronyms	Add CIS - Center for Internet Security	