#	Organization	Commentor	Type	Page #	Line #	Section	Comment (Include rationale for comment)	Suggested change
1	API	ITSS	G	NA	NA	NA	The document throughout describes the Categories and Subcategories as "outcomes" which implies that the action can be (always) completed. As this is not always the case, we recommend use of the term "objective" rather than "outcome" as this sets a goal to continuosly strive toward.	Recommend replacing "outcome" with "objective" throughout the document. See comments (5, 6, 8, 9, 10, 11, 12, 13, 14, 21, 22, 23, 24, 29, 30, 31, and 32) for specific pages/lines to change.
2	API	ITSS	E	NA	NA	NA	Not all of the informative reference are available without cost. To facilitate use, the governemnt should consider purchasing and distributing licenses to make the content available to critical infrastructure. Alternatively, read-only copies of the material, perhaps through government-sponsored "reading rooms," could be made available.	
3	API	ITSS	E	NA	NA	NA	The framework references prioritization through risk management but provides no guidance as to what constitutes a rational approach to risk management. The framework should link to guidance as to how to effectively implement risk management because a poor risk management program will likely result in insufficient security and critical infrastructure at risk.	
4	API	ITSS	G	i	3 - 5	NA	The introductory paragraph states the obvious and should be deleted. If we are reading the document, then we already know the framework is availbale for comment and as line 6 specifies NIST's involvement, there is no need for an explicit sentence on this point.	Delete these lines

5	API	ITSS	G	5	224	2.1	The Framework describes the Categories and Subcategories as “outcomes”…we would like the description to state that these are “objectives" since we cannot expect that each element can be achieved all of the time as "outcome" implies.	**Categories** are the subdivisions of a Function into groups of cybersecurity objectives.
6	API	ITSS	G	5	227	2.1	The Framework describes the Categories and Subcategories as “outcomes”…we would like the description to state that these are “objectives" since we cannot expect that each element can be achieved all of the time as "outcome" implies.	**Subcategories** further subdivide a Category into high-level objectives.
7	API	ITSS	G	6	238	2.1	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. The Framework Core should be updated with additional columns to (1) allow companies to document the standards, guidelines and practices they (will) implement to meet the objectives for each Category/Sub-Category and (2) allow companies to document any gaps they identify and prioritize which to address first.	**Company Adopted Practice**s are standards, guidelines, practices, and controls selected by the company to address the specific activity. **Gaps** are differences between company adopted practicies and implementation **Prioritzation** is a ranking indicating which gaps to close first.
8	API	ITSS	G	6	245	2.1	The Framework describes the Categories and Subcategories as “outcomes”…we would like the description to state that these are “objectives" since we cannot expect that each element can be achieved all of the time as "outcome" implies.	The Identify Function includes the following categories of objectives:

9	API	ITSS	G	7	255	2.1	The Framework describes the Categories and Subcategories as “outcomes”…we would like the description to state that these are “objectives" since we cannot expect that each element can be achieved all of the time as "outcome" implies..	The Protect Function includes the following categories of objectives:
10	API	ITSS	G	7	261	2.1	The Framework describes the Categories and Subcategories as “outcomes”…we would like the description to state that these are “objectives" since we cannot expect that each element can be achieved all of the time as "outcome" implies.	The Detect Function includes the following categories of objectives:
11	API	ITSS	G	7	268	2.1	The Framework describes the Categories and Subcategories as “outcomes”…we would like the description to state that these are “objectives" since we cannot expect that each element can be achieved all of the time as "outcome" implies..	The Respond Function includes the following categories of objectives:
12	API	ITSS	G	7	276	2.1	The Framework describes the Categories and Subcategories as “outcomes”…we would like the description to state that these are “objectives" since we cannot expect that each element can be achieved all of the time as "outcome" implies.	The Recover Function includes the following categories of objectives:
13	API	ITSS	G	7	288	2.1	The Framework describes the Categories and Subcategories as “outcomes”…we would like the description to state that these are “objectives" since we cannot expect that each element can be achieved all of the time as "outcome" implies..	The Current Profile indicates the cybersecurity objectives that are currently being achieved.

14	API	ITSS	G	7	289	2.1	The Framework describes the Categories and Subcategories as “outcomes”…we would like the description to state that these are “objectives" since we cannot expect that each element can be achieved all of the time as "outcome" implies.	The Target Profile indicates the objectives needed to achieve the desired cybersecurity risk management goals.
15	API	ITSS	G	7	294	2.2	The Framework identifies “gaps” as being differences between a company’s “Current Profile” and its “Target Profile”. Gaps should be seen as the difference between the controls adopted by a company and the controls actually implemented.	Identifying the gaps between controls adopted and those implemented allows the creation of a prirotized roadmap that organizations will implement to reduce cybersecurity risk.
16	API	ITSS	G	9	321	2.4	The Framework describes a set of “Implementation Tiers” in general terms, but fails to define how an organization would actually determine within which tier it is for each of the five “Functions”. This is not of much importance if the framework is intended only for internal use within a company but without a common (understood) "scoring" structure, there will be great variability as to how companies score themselves and no ability to effectively compare profiles among companies. A sector approach (where the sector defines tier measurement criteria) would allow valid comparisons within the sector but may not allow for cross-sector comparisons.	Consider documenting the minimum. Categories/Subcategories that must be met for each implementation Tier or at least rank the Categories/Subcategories by importance. Alternatively, sectors may recommend ranking of the categories/subcategories that are implemented to reach specific tiers for their sectors.

17	API	ITSS	G	9	321	2.4	The Framework lacks an ability to calcuate an single overall implementation tier score. Most benchmark/maturity models provide an ability to calculate a single score representaing the company's overall security posture. This number is generally what would be used to communciate the results of the survey/assessment rather than listing the scores within each area or domain. (This is similar in concept to the use of "grade point average" to reflect the posture of a student rather than listing his/her grades in each subject.) The Framework does not document how a company could calculate such an overall Implementation Tier ranking.	Consider specifying a means for calculating a summary tier level, like a numeric average of the Tier for the five Functions.
18	API	ITSS	G	9	332	2.4	Starting with "Tier 1" is a positive as it shows that an entity has done something even if minimally. The implicit "Tier 0" then is reserved for those with no security activities.	
19	API	ITSS	T	9 - 11	332 - 385	2.4	The tiers are delineated by implementing different activities within areas of risk management processes, integrated program, and external participation. Written as text, it is difficult for the reader to discern the differences between tier activities within a category; that is, it is difficult to see what the differences are between risk management processes at Tier 1, Tier 2, and Tier 3.	Consider placing these definitions into a table so one can easily see / review the differences between risk management processes, integrated program, and external participation at the different tier levels.
20	API	ITSS	T	10	345-346	2.4	There is not much differentiation between the Tier 1 and Tier 2 descriptions of "External Participation"	Replace the Tier 1 description (lines 345-346) with "The organization is uninformed of relevant industry channels for external collaboration."

21	API	ITSS	G	11	401	3.1	The Framework describes the Categories and Subcategories as “outcomes”…we would like the description to state that these are “objectives" since we cannot expect that each element can be achieved all of the time as "outcome" implies.	Organizations should have at least basic capabilities implemented in each of these areas, and can begin to review what particular categories and subcategories they currently use to help achieve those objectives.
22	API	ITSS	G	11	416	3.2	The Framework describes the Categories and Subcategories as “outcomes”…we would like the description to state that these are “objectives" since we cannot expect that each element can be achieved all of the time as "outcome" implies.	…the organization develops a Current Profile that reflects its understanding of its current cybersecurity objectives based on its implementation of the Identify Function.
23	API	ITSS	G	12	424	3.2	The Framework describes the Categories and Subcategories as “outcomes”…we would like the description to state that these are “objectives" since we cannot expect that each element can be achieved all of the time as "outcome" implies.	The organization creates a Target Profile that focuses on the assessment of the Framework Elements (e.g. Categories, Subcategories) describeing the organization's desired cybersecurity objectives.
24	API	ITSS	G	12	428	3.2	The Framework describes the Categories and Subcategories as “outcomes”…we would like the description to state that these are “objectives" since we cannot expect that each element can be achieved all of the time as "outcome" implies.	The organization creates a prioritized action plans that draws upon mission drivers, a cost/benefit analysis, and understanding of risk to achieve the objectives in the Target Profile.
25	API	ITSS	T	12	451 - 456	3.2	Besides creating new informative references, organizations can map their own existing ones into the framework.	Alternatively, an organization may have internal standards or processes which could be mapped into the framework as informative references.
26	API	ITSS	T	12	456	new section	The Framework needs to define "adoption". Recommend adding a new section to explain what constitutes "adoption".	**3.5 Adopting the Framework:** Adoption of the framework means that one has identified those practices it plans to implement to meet the Framework’s objectives and conducted a gap analysis to identify which have been implemented and which need to be improved.
27	API	ITSS	G	28 - 35	485 - 492	App. B	Privacy and civil liberties additions (Appendix B) should be integrated into the core framework	Change "Methodology" to "Sub-category" and merge privacy/civil liberties elements into core framework

28		ITSS	E	28	491	App B	The verb "implicate" generally means that the subject is connected to something else, usually in a criminal sense. Cybersecurity measures are not "criminal" so the verb would seem to be misused in this sentence.	Identify Governance - ii) Any cybersecurity measures that may induce activities, for example, interception of electronic communications under the Electronic Communications Privacy Act, or other civil liberties considerations.
29	API	ITSS	G	41	679	App. D	The Framework describes the Categories and Subcategories as “outcomes”…we would like the description to state that these are “objectives" since we cannot expect that each element can be achieved all of the time as "outcome" implies.	Focus on objectives
30	API	ITSS	G	42	702	App. E	The Framework describes the Categories and Subcategories as “outcomes”…we would like the description to state that these are “objectives" since we cannot expect that each element can be achieved all of the time as "outcome" implies.	Framework Core: an objective-based compilation of cybersecurity activities and references that are common across critical infrastructure sectors.
31	API	ITSS	G	42	708	App. E	The Framework describes the Categories and Subcategories as “outcomes”…we would like the description to state that these are “objectives" since we cannot expect that each element can be achieved all of the time as "outcome" implies.	Framework Profile: A representation of the objectives that a particular system or organization has achieved or is expected to achieve as specified in the Framework Categories and Subcategories.
32	API	ITSS	G	43	739	App. E	The Framework describes the Categories and Subcategories as “outcomes”…we would like the description to state that these are “objectives" since we cannot expect that each element can be achieved all of the time as "outcome" implies.	Subcategory: The subdivision of a Category into high-level objectives.
33	API	ITSS	E	19	NA	PR.IP-1	Process Control/SCADA systems are referred to as ICS (Industrial Control Systems) in the text of the framework document but in the core, the term "operational technology systems" appears. ICS should continue to be used rather than introducing a new term.	PR-IP-1: A baseline configuration of information technology/industrial control systems is created

34	API	ITSS	E	21	NA	PR.PR-2	"R" in "Removable" is needlessly in bold font.	Enter the "R" of "Removable" in normal text
35	API	ITSS	E	22	NA	DE-AE-1:	"A" in "A baseline..." is needlessly in bold font.	Enter the "A" of "A baseline.." in normal text
36	API	ITSS	T	24	NA	RS.AN	Need a sub-category under Respond/Analysis regarding preservation of evidence during the incident investigation.	RS.AN-4: Digital evidence identified/accumulated during the investigation must be preserved.
37	API	ITSS	E	25	NA	RS.MI-2	It is not possible to "eradicate", completely wipe out, incidents. One can manage or mitigate the event but not eradicate.	RS.MI-2: Incidents are managed/mitigated.