Comment #	Submitted By (Name/Org):*	Type (General / Editorial / Technical)	Starting Page # *	Line #	Comment (include rationale)*	Suggested Change*
1	Google	Technical	1	77	Connect the second and third paragraph of the Executive Summary for readability. Restructure sentence for fluency.	**Modify**: "The NIST Cybersecurity Framework (Framework or CSF) 2.0 provides guidance for reducing cybersecurity risks by helping organizations to understand, assess, prioritize, and communicate about those risks and the actions that will reduce them. Those actions are intended to address cybersecurity outcomes described within the CSF Core." **To**: "**The NIST Cybersecurity Framework (Framework or CSF) 2.0 provides guidance for organizations to understand, assess, prioritize, and communicate about reducing cybersecurity risks. The CSF Core describes optimal cybersecurity outcomes and the actions that organizations can take to achieve them.** **~~Those actions are intended to address cybersecurity outcomes described within the CSF Core~~**."
2		General	1	77	Add definition for "CSF Core". Mentions of "CSF Core" do not explain what the Core is or differentiate it from other CSF elements.	Explicitly define CSF Core within the document.
3		Editorial	1	78	Replace "can be understood by" with "are meant for" since a document cannot assert that its audience will understand it.	**Modify**: "These high-level outcomes can be understood by a broad audience, including executives, government officials, and others who may not be cybersecurity professionals." **To**: "These high-level outcomes **are meant for ~~can be understood by~~** a broad audience, including executives, government officials, and others who may not be cybersecurity professionals."
4		Editorial	1	79	Delete "sector- and technology-neutral" since the word "flexibility" mentioned later in the sentence implies a wide diversity of organizations and the ability to select resources.	**Modify**: "The outcomes are sector- and technology-neutral, so they provide organizations with the flexibility needed to address their unique risk, technology, and mission considerations." **To**: "The outcomes **~~are sector- and technology-neutral, so they~~** provide organizations with the flexibility needed to address their unique risk, technology, and mission considerations."
5		Technical	1	92	Remove "should" as it could imply to readers that the CSF cannot be used as a standalone document without other resources. Indicate the CSF covers many security aspects, but it is not exhaustive.	**Modify**: "The CSF should be used in conjunction with other resources (e.g., frameworks, standards, guidelines, and leading practices) to better manage cybersecurity risks and to inform overall management of cybersecurity and other risks at an enterprise level." **To**: "The CSF ~~should~~ **covers many aspects of security, but it is intended to** be used in conjunction with other resources (e.g., frameworks, standards, guidelines, and leading practices) to better manage cybersecurity risks and to inform overall management of cybersecurity and other risks at an enterprise level."
6		Editorial	2	99	Replace "is not a one-size-fits-all" with "provides a flexible" for readability.	**Modify**: "The voluntary Framework is not a one-size-fits-all approach to managing cybersecurity risks." **To**: "The voluntary Framework **~~is not a one-size-fits-all~~ provides a flexible** approach to managing cybersecurity risks."

7		Editorial	2	99	The phrase "will continue to" is unnecessary and should be removed.	**Modify**: "Organizations will continue to have unique risks — including different threats, vulnerabilities, and risk tolerances, as well as unique mission objectives and requirements across sectors." **To**: "Organizations ~~**will continue to**~~ have unique risks — including different threats, vulnerabilities, and risk tolerances, as well as unique mission objectives and requirements across sectors."
8		Technical	2	99	Organizations treat risks/threats differently, and their particular weighting of different risks/threats should be acknowledged. Grammar improvements.	**Modify**: "Organizations will continue to have unique risks — including different threats, vulnerabilities, and risk tolerances, as well as unique mission objectives and requirements across sectors." **To**: "Organizations ~~**will continue to**~~ have unique risks **depending on their particular weighting of** different threats, vulnerabilities, ~~**and**~~ risk tolerances, ~~**as well as**~~ unique mission objectives and requirements across sectors."
9		Editorial	2	108	Restructure sentence for readability.	**Modify**: "Determine where an organization may have cybersecurity gaps, including with respect to existing or emerging threats or technologies, and assess progress toward addressing those gaps." **To**: "Determine where an organization may have cybersecurity **gaps with existing and emerging threats and technologies** and assess progress toward addressing those gaps."
10		Technical	2	111	Bullet 3 more closely relates to the "Prioritize" section. "Align" suggests a prioritization sub-action, not just understanding/assessment.	**Move bullet from "Understand and Assess" to "Prioritize" section**: "Align policy, business, and technological approaches to managing cybersecurity risks across an entire organization or in a more focused area, such as a portion of the organization, a specific technology, or technology suppliers."
11		Technical	3	133	Remove 'increasing revenue' text. Risk reduction doesn't directly or consistently increase revenue and can be misleading to readers. Replace with increased customer trust, increased observability, and developer velocity.	**Modify**: "While many cybersecurity risk management activities focus on conditions that may prevent mission objectives from being achieved, it is important to also note conditions that may enable or accentuate mission achievement. Actions to reduce cybersecurity risk might benefit the organization in other ways, like increasing revenue (e.g., offering excess facility space to a commercial hosting provider for hosting their own and other organizations' data centers, then moving a major financial system from the organization's in-house data center to the hosting provider to reduce cybersecurity risk)." **To**: "While many cybersecurity risk management activities focus on conditions that may prevent mission objectives from being achieved, it is important to also note conditions that may enable or accentuate mission achievement. Actions to reduce cybersecurity risk might benefit the organization in other ways~~**, like increasing revenue**~~ (e.g., ~~**offering excess facility space to a commercial hosting provider for hosting their own and other organizations' data centers, then moving a major financial system from the organization's in-house data center to the hosting provider to reduce cybersecurity risk)**~~ **such as, increased customer trust, increased observability, and developer velocity.**"
12		Technical	3	139	Replace the three listed types of technology with "technologies". The framework can apply to other types of information and communication technologies and using an umbrella term like "technologies" ensures they are all included.	**Modify**: "The Framework applies to all information and communications technology (ICT), including information technology (IT), the Internet of Things (IoT), and operational technology (OT) used by an organization." **To**: "The Framework applies to all information and communications ~~technology (ICT), including information technology (IT), the Internet of Things (IoT), and operational technology (OT)~~ **technologies** used by an organization."

13		Technical	4	177	Define outcomes based on their alignment with maturity level objectives.	Add references to the framework tiers descriptions in Appendix B: "The Tiers characterize the typical rigor of the cybersecurity risk governance and management practices throughout an organization, including third-party cybersecurity risks."
14		Technical	5	188	Modify Fig. 1. Cybersecurity Framework Core to align with Fig. 2. Framework Functions.	Shift "Govern" from a horizontal row to a vertical column spanning the other five function rows on the left side of the graphic.
15		Technical	5	194	Replace "will" with "can". "Will" is binary while "can" implies an organization can make an attempt or be partially successful, etc.	**Modify**: "The GOVERN Function is cross-cutting and provides outcomes to inform how an organization will achieve and prioritize the outcomes of the other five Functions in the context of its mission and stakeholder expectations." **To**: "The GOVERN Function is cross-cutting and provides outcomes to inform how an organization **~~will~~ can** achieve and prioritize the outcomes of the other five Functions in the context of its mission and stakeholder expectations."
16		Technical	5	195	An organization's business goals provide the same level of important context as an organization's mission and stakeholder expectations.	**Modify**: "The GOVERN Function is cross-cutting and provides outcomes to inform how an organization will achieve and prioritize the outcomes of the other five Functions in the context of its mission and stakeholder expectations." **To**: "The GOVERN Function is cross-cutting and provides outcomes to inform how an organization will achieve and prioritize the outcomes of the other five Functions in the context of its mission**, business goals** and stakeholder expectations."
17		Technical	5	200	Add additional text at the end of the section derived from the definition of governance by the OECD; it includes the set of relationships between an organization's management, board and other stakeholders and provides a structure through which these objectives are set. Frequently, different stakeholders have different priorities, and these priorities may affect the cybersecurity strategy. For example, the shareholders of a company may be interested more in increasing the profits, and less on the security posture. On the other hand, the executive board may have cybersecurity as a high priority. Governance should define these relationships to achieve the objectives.	**Modify**: "GOVERN directs an understanding of organizational context; the establishment of cybersecurity strategy and cybersecurity supply chain risk management; roles, responsibilities, and authorities; policies, processes, and procedures; and the oversight of cybersecurity strategy." **To**: "GOVERN directs an understanding of organizational context; the establishment of cybersecurity strategy and cybersecurity supply chain risk management; roles, responsibilities, and authorities; policies, processes, and procedures; and the oversight of cybersecurity strategy. **It includes the set of relationships between an organization's management, board and other stakeholders and provides a structure through which these objectives are set**."
18		Technical	5	203	To identify the risks the reader needs to be aware of the potential adversaries. For example, a completely offline system does not have any threats coming from the internet.	**Modify**: "Understanding its assets (e.g., data, hardware, software, systems, facilities, services, people) and the related cybersecurity risks enables an organization to focus and prioritize its efforts in a manner consistent with its risk management strategy and the mission needs identified under GOVERN." **To**: "Understanding its assets (e.g., data, hardware, software, systems, facilities, services, people), **the potential adversaries** and the related cybersecurity risks enables an organization to focus and prioritize its efforts in a manner consistent with its risk management strategy and the mission needs identified under GOVERN."

19		Technical	6	208	To identify the risks the reader needs to be aware of the potential adversaries.	**Modify**: "Use safeguards to prevent or reduce cybersecurity risk. Once assets and risks are identified and prioritized, PROTECT supports the ability to secure those assets to prevent or lower the likelihood and impact of adverse cybersecurity events." **To**: "Use safeguards to prevent or reduce cybersecurity risk. Once assets**, adversaries** and risks are identified and prioritized, PROTECT supports the ability to secure those assets to prevent or lower the likelihood and impact of adverse cybersecurity events."
20		Technical	6	214	Transferring the risk (e.g., by getting cyber liability insurance), is a common practice. Note that this framework tries to address business concerns as well. Moreover, this inclusion aligns with the standard practice of avoid/mitigate/transfer/accept as well.	**Modify**: "Outcomes covered by this Function include awareness and training; data security; identity management, authentication, and access control; platform security (i.e., securing the hardware, software, and services of physical and virtual platforms); and the resilience of technology infrastructure." **To**: "Outcomes covered by this Function include awareness and training; data security; identity management, authentication, and access control; platform security (i.e., securing the hardware, software, and services of physical and virtual platforms); the resilience of technology infrastructure**; and the transfer of risk**."
21		Technical	6	215	Include "denoise" alongside "find" and "analyze". Denoise differentiates false positives from false negatives which are a critical problem here.	**Modify**: "*Find and analyze possible cybersecurity attacks and compromises.*" **To**: "*Find* ***, denoise,*** *and analyze possible cybersecurity attacks and compromises* ."
22		Technical	6	218	Post factum detection of incidents is a valid objective of detection. "Timely discovery" is not just real-time.	**Modify**: "Find and analyze possible cybersecurity attacks and compromises. DETECT enables timely discovery and analysis of anomalies, indicators of compromise, and other potentially adverse cybersecurity events that may indicate that cybersecurity attacks and incidents are occurring." **To**: "Find and analyze possible cybersecurity attacks and compromises. DETECT enables timely discovery and analysis of anomalies, indicators of compromise, and other potentially adverse cybersecurity events that may indicate that cybersecurity attacks and incidents are occurring **or have occured**."
23		Technical	8	277	Indicate clearly that the organizational leadership sets risk appetite and tolerance. Remove "as outlined in GOVERN" as it is unnecessary.	**Modify**: "With an understanding of stakeholder expectations and risk appetite and tolerance (such as outlined in GOVERN), organizations can prioritize cybersecurity activities, enabling them to make informed decisions about cybersecurity expenditures and actions." **To**: "With an understanding of stakeholder expectations, risk appetite and tolerance (**which are set by the organization's leadership~~ as outlined in GOVERN~~**), organizations can prioritize cybersecurity activities, enabling them to make informed decisions about cybersecurity expenditures and actions."
24		Technical	8	284	Remove - restates previous paragraph.	**Remove**: "This section explains several ways that organizations can use the Framework:"
25		Editorial	8	295	The existing text is unnecessarily wordy. Replace with "The Framework helps organizations".	**Modify**: "Regardless of the application of the Framework, organizations likely will find it helpful to think of the Framework as guidance to help them to understand, assess, prioritize, and communicate about those cybersecurity risks and the actions that will reduce those risks." **To**: "**The Framework helps organizations** **~~Regardless of the application of the Framework, organizations likely will find it helpful to think of the Framework as guidance to help them to~~** understand, assess, prioritize, and communicate about those cybersecurity risks and the actions that will reduce those risks."

26		Editorial	8	297	Grammar correction.	**Modify**: "The outcomes which are selected can be used to focus on and implement strategic decisions to improve an organization’s cybersecurity posture (or state), taking into account its priorities and available resources." **To**: "The **selected** outcomes ~~**which are selected**~~ can be used to focus on and implement strategic decisions to improve an organization’s cybersecurity posture (or state), taking into account its priorities and available resources."	
27		Editorial	8	299	The term "(or state)" is unnecessary and should be removed.	**Modify**: "The outcomes which are selected can be used to focus on and implement strategic decisions to improve an organization’s cybersecurity posture (or state), taking into account its priorities and available resources." **To**: "The outcomes which are selected can be used to focus on and implement strategic decisions to improve an organization’s cybersecurity posture~~ **(or state)**~~, taking into account its priorities and available resources."	
28		Editorial	9	314	Grammar correction.	**Modify**: "A Current Profile covers the Core’s outcomes that an organization is currently achieving (or attempting to achieve) and characterizes how or to what extent each outcome is being achieved." **To**: "A Current Profile ~~**covers**~~ **describes** the Core’s outcomes that an organization is currently achieving (or attempting to achieve) and characterizes how or to what extent each outcome is being achieved."	
29		Editorial	9	315	Grammar correction.	Modify: "A Current Profile covers the Core’s outcomes that an organization is currently achieving (or attempting to achieve) and characterizes how or to what extent each outcome is being achieved." To: "A Current Profile covers the Core’s outcomes that an organization **is working toward or has achieved** by characterizing how or to what extent each outcome is being achieved."	
30		Editorial	9	317	Grammar correction.	**Modify**: "A Target Profile covers the desired outcomes that an organization has selected and prioritized from the Core for achieving its cybersecurity risk management objectives." **To**: "A Target Profile ~~**covers**~~ **describes** the desired outcomes that an organization has selected and prioritized from the Core for achieving its cybersecurity risk management objectives."	
31		Editorial	9	324	Grammar correction -- replace with "focus on new requirements"	**Modify**: "Others prefer to start with a Target Profile to work toward. For example, an organization that needs to meet a set of new requirements might focus on developing its Target Profile first and in the course of doing so, also determine its current cybersecurity posture for its Current Profile." **To**: "Others prefer to start with a Target Profile **to focus on new requirements** ~~**work toward. For example, an organization that needs to meet a set of new requirements might focus on developing its Target Profile first**~~ and in the course of doing so, also determine its current cybersecurity posture for its Current Profile."	
32		Editorial	10	329	Remove "create and" for succinctness.	**Modify**: "Organizations can create and use Profiles to utilize the full capabilities of the Framework (as discussed in Section 1)." **To**: "Organizations can~~ **create and**~~ use Profiles to utilize the full capabilities of the Framework (as discussed in Section 1)."	

33		Technical	10	330	Replace with "profiles". Organizations can make the determination to use or not use profiles on their own.	**Modify**: "While organizations can use the Framework without Profiles, they provide the opportunity to develop a prioritized roadmap to achieve the cybersecurity outcomes of the Framework." **To**: "~~**While organizations can use the Framework without**~~ Profiles~~**, they**~~ provide the opportunity to develop a prioritized roadmap to achieve the cybersecurity outcomes of the Framework."
34		Editorial	10	332	Rephrase for sentence fluency.	**Modify**: "There are many ways to use Profiles, including to:" **To**: "Organizations can use profiles to:"
35		Editorial	10	341	Grammar correction for succinctness.	**Modify**: "Determine where the organization may have cybersecurity gaps with respect to an emerging threat or a new technology" **To**: "**Identify** ~~**Determine where the organization may have**~~ cybersecurity gaps with respect to an emerging threat or a new technology"
36		Editorial	10	343	Grammar correction -- remove unnecessary text that doesn't change the meaning of the sentence.	**Modify**: "Communicate about the cybersecurity capabilities an organization provides — for example, to business partners or to prospective customers of the organization’s technology products and services" **To**: "Communicate an organization's cybersecurity capabilities ~~**about the cybersecurity capabilities an organization provides**~~ — for example, to business partners or to prospective customers of the organization’s technology products and services"
37		Technical	10	354	Modify Fig. 4. Steps for creating and using Cybersecurity Framework Profiles for reader understanding.	The steps in the graphic would make more sense as a circle (as opposed to up or down) if it is supposed to be representative of continuous improvement efforts (e.g. the arrows should only have one direction rather than being bilateral).
38		Technical	11	364	Gathering relevant resources should be recommended whenever organizations prepare profiles.	**Modify**: "An organization can gather relevant resources prior to preparing the Profiles, such as organizational policies, risk management priorities and resources, cybersecurity requirements and standards followed by the organization, and work roles." **To**: "An organization ~~**can**~~ **should** gather relevant resources prior to preparing the Profiles, such as organizational policies, risk management priorities and resources, cybersecurity requirements and standards followed by the organization, and work roles."
39		Editorial	11	367	Grammar correction for succinctness.	**Modify**: "Understanding cybersecurity governance — such as identifying the organization’s mission, its stakeholders, and their needs and expectations, as outlined in the GOVERN Function — is generally needed for preparing a Target Profile." **To**: "Understanding cybersecurity governance — **including** ~~**such as identifying**~~ the organization’s mission, its stakeholders, and their needs and expectations, as outlined in the GOVERN Function — is generally needed for preparing a Target Profile."

40		Editorial	12	401	"For example," is unnecessary and can be removed.	**Modify**: "For example, Profile developers can reach out to leaders within the organization to confirm which resources (e.g., facilities, personnel, systems) are most relevant to achieving the objectives (e.g., for a business unit)." **To**: "~~**For example,**~~ Profile developers can reach out to leaders within the organization to confirm which resources (e.g., facilities, personnel, systems) are most relevant to achieving the objectives (e.g., for a business unit)."
41		Technical	12	408	Federated responsibility guidance for advanced (or enterprise) organizations is missing in the framework and should be included.	Add paragraph to 3.1 after line 417: "**Advanced organizations recognise responsibility for risk often is federated, and as such build a profile model that utilises inheritance and composition to implement this delegation and federation of responsibility. With such systems, high level teams such as the CISO team can mandate an org-wide profile target while sub-teams can implement their own additive requirements**."
42		Editorial	12	419	Remove unnecessary preface.	**Modify**: "Step 3, “Create Current and Target Profiles” in Section 3.1 mentions that creating Profiles means filling in the elements for each selected Core outcome." **To**: "~~**Step 3, “Create Current and Target Profiles” in Section 3.1 mentions that creating**~~ **Creating** Profiles means filling in the elements for each selected Core outcome.
43		Editorial	13	451	Restructure for sentence fluency.	**Modify**: "Tiers characterize the rigor of an organization’s cybersecurity risk governance and management outcomes, and they provide context on how an organization views cybersecurity risks and the processes in place to manage those risks." **To**: "Tiers characterize the rigor of an organization’s cybersecurity risk governance and management outcomes, **the organization's views of cybersecurity risks**~~**, and they provide context on how an organization views cybersecurity risks**~~ and the processes in place to manage those risks."
44		Editorial	13	455	Grammar correction for succinctness.	**Modify**: "The Tiers capture an organization’s outcomes over a range, from Partial (Tier 1) to Adaptive (Tier 4), as Fig. 5 depicts." **To**: "The Tiers **range** ~~**capture an organization’s outcomes over a range,**~~ from Partial (Tier 1) to Adaptive (Tier 4), as Fig. 5 depicts."
45		Technical	13	456	Fig. 5. should be removed -- the height of the bars are abstract and the figure shows only a bulleted list as a visual.	Remove Fig. 5. Cybersecurity Framework Tiers.
46		Editorial	13	460	Grammar correction for succinctness.	**Modify**: "For example, an organization can use the Tiers to communicate internally as a benchmark for a more organization-wide approach to managing cybersecurity risks as necessary to progress to a higher Tier." **To**: "For example, an organization can use the Tiers to **establish** ~~**communicate internally as**~~ a benchmark for a more organization-wide approach to managing cybersecurity risks as necessary to progress to a higher Tier."

47		Technical	14	482	This title is unnecessarily descriptive. The subsection titles should have more detail while the overarching section title should be broader (and shorter).	**Modify**: "3.4 Improving Communication With Internal and External Stakeholders Using the Framework" **To**: "3.4 Improving Communication **about Security** **~~With Internal and External Stakeholders Using the Framework~~**"
48		Editorial	14	485	Grammar correction for sentence fluency.	**Modify**: "One of the most common benefits of using the Framework is improving communication regarding cybersecurity risks and posture with those inside and outside of an organization." **To**: "One of the most common benefits of using the Framework is improving communication **about** **~~regarding~~** cybersecurity risks and posture with those inside and outside of an organization."
49		Editorial	14	486	Grammar correction for sentence fluency.	**Modify**: "This section explains how to use the Framework to facilitate communication and discusses many of the entities that may benefit." **To**: "This section explains how to use the Framework to **guide such** **~~facilitate~~** communication and discusses many of the entities that may benefit."
50		Editorial	15	501	As this sentence aims to state the action is on the senior executive to approve the tier selection, "will" should be added before "approve".	**Modify**: "When implementing the Framework, the senior executive level will focus on organizational risk, with actions to express mission priorities under the GOVERN Function and approve Framework Tier selection." **To**: "When implementing the Framework, the senior executive level will focus on organizational risk, with actions to express mission priorities under the GOVERN Function and **will** approve Framework Tier selection."
51		Technical	15	509	Replace current text with "both influenced by and impact processes and objectives at various levels of the business or governmental entity." Adding the word "levels" takes into consideration the various strata of the applicable entity.	**Modify**: "The overall cybersecurity objectives set at the senior executive level are informed by and cascade to specific business process level objectives. In a commercial entity, these may apply to a line-of-business or operating division. For government entities these may be division- or branch-level considerations." **To**: "The overall cybersecurity objectives set at the senior executive level are **both influenced by and impact processes and objectives at various levels of the business or governmental entity** **~~informed by and cascade to specific business process level objectives. In a commercial entity, these may apply to a line-of-business or operating division. For government entities these may be division- or branch-level considerations~~**."
52		Editorial	15	516	Grammar correction for sentence fluency.	**Modify**: "As risk priorities and appetite are translated into mission-level objectives, business process managers can express their own cybersecurity expectations and performance criteria in terms of how uncertainty created by risk may impact the business." **To**: "As risk priorities and appetite are translated into mission-level objectives, business process managers can express their own cybersecurity expectations and performance criteria **taking into consideration business risk** **~~in terms of how uncertainty created by risk may impact the business~~**."
53		Editorial	16	551	Grammar correction for sentence fluency.	**Modify**: "All types of technology rely on a complex, globally distributed, extensive, and interconnected supply chain ecosystem with geographically diverse routes and multiple levels of outsourcing." **To**: "**Many technologies** **~~All types of technology~~** rely on a complex, globally distributed, extensive, and interconnected supply chain ecosystem with geographically diverse routes and multiple levels of outsourcing."

54		Editorial	16	552	Grammar correction for sentence fluency.	**Modify**: "All types of technology rely on a complex, globally distributed, extensive, and interconnected supply chain ecosystem with geographically diverse routes and multiple levels of outsourcing." **To**: "All types of technology rely on a complex, global**~~ly distributed, extensive,~~** and interconnected supply chain ecosystem with geographically diverse routes and multiple levels of outsourcing."
55		Editorial	16	553	The word "geographically" is unnecessary since "global" has already been used.	**Modify**: "All types of technology rely on a complex, globally distributed, extensive, and interconnected supply chain ecosystem with geographically diverse routes and multiple levels of outsourcing." **To**: "All types of technology rely on a complex, globally distributed, extensive, and interconnected supply chain ecosystem with **~~geographically~~** diverse routes and multiple levels of outsourcing."
56		Editorial	16	554	Grammar correction for sentence fluency and succinctness.	**Modify**: "This ecosystem is composed of public- and private-sector entities (e.g., acquirers, suppliers, developers, system integrators, external system service providers, and other technology-related service providers) that interact to research, develop, design, manufacture, acquire, deliver, integrate, operate, maintain, dispose of, and otherwise utilize or manage technology products and services." **To**: "This ecosystem is composed of public- and private-sector entities **such as acquirers, suppliers, and service providers ~~(e.g., acquirers, suppliers, developers, system integrators, external system service providers, and other technology-related service providers)~~** that interact to research, develop, design, manufacture, acquire, deliver, integrate, operate, maintain, dispose of, and otherwise utilize or manage technology products and services."
57		Editorial	16	555	Grammar correction for sentence fluency and succinctness.	**Modify**: "This ecosystem is composed of public- and private-sector entities (e.g., acquirers, suppliers, developers, system integrators, external system service providers, and other technology-related service providers) that interact to research, develop, design, manufacture, acquire, deliver, integrate, operate, maintain, dispose of, and otherwise utilize or manage technology products and services." **To**: "This ecosystem is composed of public- and private-sector entities (e.g., acquirers, suppliers, developers, system integrators, external system service providers, and other technology-related service providers) **work together to research, develop, manage, and use ~~that interact to research, develop, design, manufacture, acquire, deliver, integrate, operate, maintain, dispose of, and otherwise utilize or manage~~** technology products and services."
58		Editorial	17	565	Grammar correction for sentence fluency and succinctness.	**Modify**: "Today, nearly all organizations depend on supply chains. As such, it is increasingly important that they develop capabilities and implement practices to identify, assess, and respond to cybersecurity risks throughout the supply chain." **To**: "**It is important for organizations to ~~Today, nearly all organizations depend on supply chains. As such, it is increasingly important that they~~** develop capabilities and implement practices to identify, assess, and respond to cybersecurity risks throughout the supply chain."
59		Editorial	17	568	Grammar correction for sentence fluency and succinctness.	**Modify**: "The primary objective of C-SCRM is to extend appropriate first-party cybersecurity risk management considerations to third parties, supply chains, and products and services an organization acquires, based on supplier criticality and risk assessment." **To**: "The primary objective of C-SCRM is to extend appropriate first-party cybersecurity risk management considerations to **the supply chain ~~third parties, supply chains, and products and services an organization acquires,~~** based on supplier criticality and risk assessment."
60		Editorial	17	570	The word "potentially" is redundant when it follows the word "may".	**Modify**: "Examples of risks include products and services that may potentially contain or become a vector for malicious functionality, are counterfeit, or are vulnerable due to poor manufacturing and development practices within the supply chain." **To**: "Examples of risks include products and services that may **~~potentially~~** contain or become a vector for malicious functionality, are counterfeit, or are vulnerable due to poor manufacturing and development practices within the supply chain."

61		Editorial	17	579	Grammar correction for sentence fluency and succinctness.	**Modify**: "The Framework Core addresses cybersecurity supply chain risk management in two ways. Within the GOVERN function, the Supply Chain Risk Management (GV.SC) Category and its Subcategories provide outcomes for establishing, managing, monitoring, and improving an organizational cybersecurity supply chain risk management capability or program." **To**: "The Framework Core addresses cybersecurity supply chain risk management in two ways. Within the GOVERN function, the Supply Chain Risk Management (GV.SC) Category and its Subcategories provide outcomes **that inform** ~~**for establishing, managing, monitoring, and improving**~~ an organizational cybersecurity supply chain risk management capability or program."
62		Editorial	18	607	Replace "delineate" with "identify" since it is more commonly used and recognized.	**Modify**: "An organization can use Framework Profiles to delineate cybersecurity standards and practices to incorporate into contracts with suppliers and provide a common language to communicate those requirements to suppliers." **To**: "An organization can use Framework Profiles to **identify** ~~**delineate**~~ cybersecurity standards and practices to incorporate into contracts with suppliers and provide a common language to communicate those requirements to suppliers."
63		Editorial	18	611	Grammar correction for sentence fluency and succinctness.	**Modify**: "Target Profiles can be used to inform decisions about buying products and services based on requirements to address gaps." **To**: "Target Profiles can ~~**be used to**~~ inform decisions about buying products and services based on requirements to address gaps."
64		Editorial	18	614	The word "supplier" is unnecessary as suppliers are inherently considered apart of the supply chain.	**Modify**: "This often entails some degree of trade-off with other requirements, comparing multiple products or services and considering other needs such as cost, functionality, and supplier and supply chain risks." **To**: "This often entails some degree of trade-off with other requirements, comparing multiple products or services and considering other needs such as cost, functionality, ~~**and supplier**~~ and supply chain risks."
65		Editorial	18	630	This action can happen at all levels -- it is unnecessary to indicate the specific level in the sentence.	**Modify**: "Some organizations integrate all of their risk management efforts at a high level by using enterprise risk management (ERM)." **To**: "Some organizations integrate all of their risk management efforts ~~**at a high level**~~ by using enterprise risk management (ERM)."
66		Editorial	18	634	Grammar correction for sentence fluency and succinctness.	**Modify**: "The outer border of Fig. 7 indicates an organization's full range of ERM risks, with examples of risks including financial, legal, operational, physical security, reputational, and safety — in addition to cybersecurity and privacy risks." **To**: "The outer border of Fig. 7 indicates an organization's full range of ERM risks, ~~**with examples of risks**~~ including financial, legal, operational, physical security, reputational, and safety — in addition to cybersecurity and privacy risks."
67		Technical	20	680	The processes mentioned can be implemented both inside and outside the organization.	**Modify**: "Put processes in place to assess and address whether, when, how, and the extent to which individuals' data is shared outside of the organization as part of cybersecurity information-sharing activities" **To**: "Put processes in place to assess and address whether, when, how, and the extent to which individuals' data is shared ~~**outside of the organization**~~ as part of cybersecurity information-sharing activities"

68		Editorial	21	698	Change 3.1 to 3.1.2 - "3.1.2. Steps for Creating and Using Profiles" for accuracy/specificity.	**Modify**: "Section 3.1 of this document presents five steps that an organization could take using Framework Profiles to help inform continuous improvement of its cybersecurity posture." **To**: "~~Section 3.1~~ **3.1.2. Steps for Creating and Using Profiles** of this document presents five steps that an organization could take using Framework Profiles to help inform continuous improvement of its cybersecurity posture."
69		Editorial	21	700	Grammar correction for sentence fluency and succinctness.	**Modify**: "Organizations can expand and enhance those steps to integrate ERM considerations, such as:" **To**: "Organizations can expand and enhance those steps to integrate ERM considerations~~, such as~~:"
70		Technical	21	702	Remove "Step _" in parentheses after each bullet. Preface each bullet with its respective fully expanded step name for readability and understanding.	**Modify**: "Ensuring that assets that are important to the enterprise are considered when defining the Framework use case (step 1)" **To**: "**Step 1. Define the use case for the Profiles:** Ensuring that assets that are important to the enterprise are considered when defining the Framework use case~~ (step 1)~~"
71		Technical	21	706	Replace "current state" with "current profile" to align with terminology used in "3.1.2 - Step 3. Create Current and Target Profiles." Replace "desired state" with "target profile" to align with terminology used in "3.1.2 - Step 3. Create Current and Target Profiles."	**Modify**: "Considering tangible and assessable representation of risks (risk scenarios) from throughout the enterprise when evaluating the risk implications of the current state and defining the desired state that will address important risks (step 3)" **To**: "Considering tangible and assessable representation of risks (risk scenarios) from throughout the enterprise when evaluating the risk implications of the ~~current state~~ **current profile** and defining the ~~desired state~~ **target profile** that will address important risks (step 3)"
72		Technical	32	725	Change section title to "Additional Recommendations". No definitive next steps are defined in this section and its current title is misleading.	**Modify**: "5. Next Steps" **To**: "5. Additional Recommendations"
73		Editorial	21	727	Grammar correction for sentence fluency and succinctness.	**Modify**: "Whether an organization is using the Cybersecurity Framework for the first time or it has used the Framework previously, it is important to remember that the CSF is designed to be used in conjunction with other cybersecurity frameworks, standards, and guidance." **To**: "Whether an organization is using the Cybersecurity Framework for the first time or it has used the Framework previously, it is important to remember that the CSF is designed to be used ~~in conjunction~~ with other cybersecurity frameworks, standards, and guidance."
74		Technical	31	ble 5GV.SC-0	Add "procurement" to support the proactive approach to supply-chain security at the point of third-party selection.	**Modify**: "Cybersecurity supply chain risk management is integrated into cybersecurity and enterprise risk management, risk assessment, and improvement processes (formerly ID.SC-02)" **To**: "Cybersecurity supply chain risk management is integrated into cybersecurity and enterprise risk management, risk assessment**, procurement** and improvement processes (formerly ID.SC-02)"

75		Technical	31	ble 5GV.SC-0	GV.SC-09 has significant overlap with GV.SC-03 and should be merged.	Merge GV.SC-03 with GV.SC-09.