#	Organization	Commenter	Type	Page #	Line #	Section	Comment (Include rationale for comment)	Suggested change
1	APPA-LPPC		T	Several	Several	Several	The EO is specifically related to the Critical Infrastructure as defined within the EO. These terms are broad and can be interpreted to mean non-critical infrastructure protection parts of critical infrastructure owners and operators	Change the business terms like 'organization,' 'mission,' business' to "Critical Infrastructure"
2	APPA-LPPC		T	Several	Several	Several	Throughout the document there is an interchanging use of the 'activities' and 'outcomes.' Ultimately the intent is that critical infrastructure owners and operators are going to achieve 'outcomes' associated with the CSF	Change 'activities' to 'outcomes' throughout the document
3	APPA-LPPC		G	1	71-76	1.0 Framework Introduction	Good to have this language from the EO in the Introduction	No change
4	APPA-LPPC		T	1	88	1.0 Framework Introduction	make sure that it is clear that we are after cyber improvements	to achieve "cybersecurity" outcomes

5	APPA-LPPC		T	1	91	1.0 Framework Introduction	need to make it clear that this is meant for critical infrastructure even with language in intro from EO	add critical infrastructure in front of business
6	APPA-LPPC		T	1	91	1.0 Framework Introduction	need to make it clear that we are leveraging existing standards but recognizing there are emerging standards	add "existing and emerging" after The use of…
7	APPA-LPPC		T	2	100	1.0 Framework Introduction		replace business with enterprise
8	APPA-LPPC		T	2	102	1.0 Framework Introduction	its not just about improving a program	change improve to measure alignment with Framework
9	APPA-LPPC		T	2	103	1.0 Framework Introduction	Add the sentence before Alternatively .	The Framework is not designed to be used by third parties to grade performance or provide a basis for any form of certification.
10	APPA-LPPC		T	2	114	1.1 Overview of the Framework	we are looking to achieve outcomes through the subcategories	change activities to outcomes
11	APPA-LPPC		E	2	114	1.1 Overview of the Framework	Making sure to connect back to the Informative References identified either in the Framework Core or selected by the sector/organization	add informative in front of references
12	APPA-LPPC		E	2	116	1.1 Overview of the Framework	Making sentence clearer that there are existing standards	add existing in front of standards

13	APPA-LPPC		E	2	123-125	1.1 Overview of the Framework	this sentence appears confusing	Remove sentence This structure ties the high-level strategic view, outcomes…
14	APPA-LPPC		T	3	143	1.1 Overview of the Framework	This is intended to make it clear that some sectors have standards that are directly applied to them.	add sector specific in front of industry standards
15	APPA-LPPC		E	3	145	1.1 Overview of the Framework	Attempting to tie back to the overall posture of cybersecurity.	add posture in front of by comparing
16	APPA-LPPC		T	3	140-149	1.1 Overview of the Framework	The Framework Core is a “baseline” meant to be cross sector. Through the creation of the first Current Profile, the organization needs to evaluate each of the Functions, Categories and Subcategories in the Framework Core. As critical infrastructure creates their Target Profile, they may need to add more categories and subcategories that might be entity or sector specific, but they should not subtract any of the Framework Core categories and subcategories from the Current Profile.	it is unclear whether a Profile could subtract categories and subcategories

17	APPA-LPPC		T	3	153	1.1 Overview of the Framework	Making sure to reiterate that this is for critical infrastructure.	add critical infrastructure in front of business/mission
18	APPA-LPPC		T	3	166	1.2 Risk Management and the Cybesecurity Framework	this is a global change to make it clear that this applies to the CI aspects of the organization	add critical infrastructure in front of organizations
19	APPA-LPPC		E	3	167	1.2 Risk Management and the Cybesecurity Framework	Rewording the sentence.	add needed in front of changes. Add their in front of organizational and delete organizational. Add programs after cybersecurity
20	APPA-LPPC		E	3	174-176	1.2 Risk Management and the Cybesecurity Framework	These statements were made at the opening of the paragraph.	remove entire opening sentence
21	APPA-LPPC		E	3	176-179	1.2 Risk Management and the Cybesecurity Framework	Examples seem to flow well being moved.	move to end of 173

22	APPA-LPPC		T	3	181	1.2 Risk Management and the Cybesecurity Framework	Adding cyber to make sure we stay connected to cybersecurity as the outcome.	add cyber in front of security
23	APPA-LPPC		E	5	203-205	2.0 Framework Basics	This statement leads the reader to be concerned about how other uses will be made with the framework.	change sentence that begins with "Different types" to say "The Framework provides critical infrastructure owners and operators the ability to create a Profile that meets the outcomes and risk management practices within their sector or within their organization.
24	APPA-LPPC		E	5	207	2.0 Framework Basics	Rewording the sentence to be more specific about informative references.	add informative in front of references and remove from end of sentence. Add "which contain existing cybersecurity practices" Change activities to outcomes
25	APPA-LPPC		E	5	209	2.0 Framework Basics	Adding clarifying word.	add "successfully" in front of manage
26	APPA-LPPC		E	5	216	2.0 Framework Basics	Adding clarification to the sentence for flow.	change the opening sentence to say "Functions provide the highest level of organization within the Framework. The five Functions are…"

27	APPA-LPPC		T	6	218	2.0 Framework Basics	the functions do not necessarily themselves provide this ability, as do the use of the Tiers and Profiles within the Framework.	remove "the state of an organization's cybersecurity activities by organizing"
28	APPA-LPPC		E	6	227	2.0 Framework Basics	The result is that these are outcomes.	remove high-level
29	APPA-LPPC		T	6	230	2.0 Framework Basics	There is a request further down to change this subcategory to be more broad and to tie to critical infrastructure data. Not all data needs to be protected at rest. It needs to be commensurate with your risk management practices	If this is the example that is to be retained, align with recommendation for the subcategory and change to: "Critical Infrastructure Data-at-rest is protected based on risk management practices"
30	APPA-LPPC		E	6	232	2.0 Framework Basics	This seems like a broad introduction of the Information References.	Change "specific sections" to "existing"
31	APPA-LPPC		E	6	235-237	2.0 Framework Basics	Rewording the sentence for clarity.	Reword the sentence beginning at "The Informative References presented…" to say "The Informative References presented in the Framework Core are a baseline set of standards, guidelines and practices. Through the use of Profiles, critical infrastructure sectors are encouraged to include other standards, guidelines, and practices that are more specific to their sector.
32	APPA-LPPC		T	6	238-241	2.0 Framework Basics	This statement seems out of place after completing the introduction of the components of the framework.	Move to a call out box or footnote.
33	APPA-LPPC		T	6	249	2.0 Framework Basics	Need to keep making it clear that this is related to critical infrastructure	Insert "infrastructure" in front of "functions"
34	APPA-LPPC		E	6	251	2.0 Framework Basics		change "or" to "of"

35	APPA-LPPC		T	6	252	2.0 Framework Basics		change "safeguards" to "outcomes"
36	APPA-LPPC		T	6	253	2.0 Framework Basics		change "delivery" to "resilience"
37	APPA-LPPC		T	7	262-264	2.0 Framework Basics	The detect function itself is not about response, but about the discovery to aid the response function.	change the sentence beginning with "The Detect Function" to read as "The Detection function enables timely discovery of cybersecurity events to limit or contain the impact of a potential cyber incident.
38	APPA-LPPC		T	7	266	2.0 Framework Basics	This is an outcome of effective risk management.	remove (including effective planning)
39	APPA-LPPC		T	7	274	2.0 Framework Basics		change "or" to "of"

40	APPA-LPPC		T	7-8	281-306	2.0 Framework Basics	This new text replaces the original text starting from line 281 and ending at line 306.	2.2 Framework Profile: A Framework Profile ("Profile") is a tool to enable organizations to establish a roadmap for reducing cybersecurity risk that is well aligned with organization and sector goals, considers legal/regulatory requirements and industry best practices, and reflects risk management priorities. A Framework Profile can be used to describe both the current state and the desired target state of specific cybersecurity activities, thus revealing gaps that can be addressed to meet cybersecurity risk management objectives. Figure 2 shows the two types of Profiles: Current and Target. The Current Profile indicates the cybersecurity outcomes that are currently being achieved. The Target Profile indicates the outcomes needed to achieve the desired cybersecurity risk management goals. The Target Profile is built to support critical infrastructure requirements and aid in the communication of risk within and between organizations.

41	APPA-LPPC		T	7-9	281-307	2.0 Framework Basics	This new text replaces the original text starting from line 281 and ending at line 306.	The Profile is the alignment of the Functions, Categories, Subcategories and industry standards with the business requirements, risk tolerance, and resources of the organization. The prioritization of the gaps is driven by the selection of the Framework Tier and organization's Risk Management Processes which can serve as an essential part for resource and time estimates needed that are critical to prioritization decisions . Figure 2: Profile Comparisons The Framework provides a mechanism for critical infrastructure organizations, sectors, and other entities to create their own Target Profiles. It does not provide Target Profile templates; rather, sectors and organizations should identify existing Target Profiles based on their risk determinations and needs.

42	APPA-LPPC			7-8	307-320	2.4 Framework Implementation Tiers	Section 2.3 is moved to Section 3.1 after line 308. The previous section 2.4 is renumbered to 2.3. This new text replaces the original text of Section 2.4 starting from line 307 and ending at line 320.	2.3 Framework Implementation Tiers: The Framework Implementation Tiers (“Tiers”) describe how an organization manages its implementation of the Framework Functions and critical infrastructure cybersecurity risk management practices. The Tiers range from Not Initiated (Tier 0) to Adaptive (Tier 4) and describe an increasing degree of rigor and institutionalization of cybersecurity risk management practices and the extent to which cybersecurity risk management is integrated into an organization’s overall risk management practices. The Tier selection process considers an organization’s current risk management practices, threat environment, legal and regulatory requirements, critical infrastructure business/mission objectives, and organizational constraints.
43	APPA-LPPC			7-9	307-321	2.4 Framework Implementation Tiers	Section 2.3 is moved to Section 3.1 after line 308. The previous section 2.4 is renumbered to 2.3. This new text replaces the original text of Section 2.4 starting from line 307 and ending at line 320.	Organizations should determine the desired Tier, ensuring that the selected levels meet the organizational goals, reduce cybersecurity risk to critical infrastructure, and are feasible and cost-effective to implement. The Tier definitions are as follows:

44	APPA-LPPC		T	8	332	2.4 Framework Implementation Tiers	A Tier 0 is created to denote that Tier 1 has not been achieved. This is useful when creating a Current Profile for those organizations that cannot note that they are at Tier 1. This also allows an organization to identify where to invest resources. This is not intended to be the Tier that an organization achieves, but rather a placeholder in a Current Profile for an organization to measure improvement to the Target Tier.	• Tier 0: Not Initiated o Tier 1 has not been achieved.

45	APPA-LPPC		T	9-10	332-346	2.4 Framework Implementation Tiers	The Tier 1 text has been modified to include the connection to the Framework Functions. This could also be said to be the Framework Core. The intent of this change is to create a tie to the Framework Profile creation process and a way for organizations to determine not only their Risk Management strategy but their institutionalization of the Framework Core to achieve greater cybersecurity.	• Tier 1: Initiated o Risk Management Process – The Framework Functions and critical infrastructure cybersecurity risk management practices are not formalized and risk is managed in an ad hoc, irregular and sometimes reactive manner. Prioritization of cybersecurity activities may not be directly informed by organizational risk objectives, the threat environment, or business/mission requirements essential for critical infrastructure.

46	APPA-LPPC		T	9-11	332-347	2.4 Framework Implementation Tiers	The Tier 1 text has been modified to include the connection to the Framework Functions. This could also be said to be the Framework Core. The intent of this change is to create a tie to the Framework Profile creation process and a way for organizations to determine not only their Risk Management strategy but their institutionalization of the Framework Core to achieve greater cybersecurity.	o Integrated Program – There is a limited awareness of cybersecurity risk at the organizational level. The organization implements cybersecurity risk management on an irregular, case-by-case basis due to varied experience or inadequate resources. o Information Sharing – The organization may not have processes that enable cybersecurity information to be shared within the organization. An organization may not have the processes in place to participate in coordination or collaboration with other entities.

47	APPA-LPPC		T	10	347-357	2.4 Framework Implementation Tiers	The Tier 2 text has been modified to include the connection to the Framework Functions. This could also be said to be the Framework Core. The intent of this change is to create a tie to the Framework Profile creation process and a way for organizations to determine not only their Risk Management strategy but their institutionalization of the Framework Core to achieve greater cybersecurity.	• Tier 2: Risk-Informed o Risk Management Process – The Framework Functions and critical infrastructure risk management practices are supported by management but may not be established as documented policy. o Integrated Program – There is an awareness of cybersecurity risk at the critical infrastructure operations level but an integrated, overall organization-wide approach to managing critical infrastructure cybersecurity risk has not been established. Risk-informed processes and procedures are identified. Cybersecurity personnel resources have been identified but may not be dedicated to or have sufficient knowledge and skills to perform their cybersecurity duties.

48	APPA-LPPC		T	11	347-358	2.4 Framework Implementation Tiers	The Tier 2 text has been modified to include the connection to the Framework Functions. This could also be said to be the Framework Core. The intent of this change is to create a tie to the Framework Profile creation process and a way for organizations to determine not only their Risk Management strategy but their institutionalization of the Framework Core to achieve greater cybersecurity.	o Information Sharing – Cybersecurity information is shared within the organization on an informal basis. The organization knows its role in critical infrastructure, but has not formalized its capabilities to interact and share information externally.

49	APPA-LPPC		T	10	358-370	2.4 Framework Implementation Tiers	The Tier 3 text has been modified to include the connection to the Framework Functions. This could also be said to be the Framework Core. The intent of this change is to create a tie to the Framework Profile creation process and a way for organizations to determine not only their Risk Management strategy but their institutionalization of the Framework Core to achieve greater cybersecurity.	• Tier 3: Risk-Informed and Repeatable o Risk Management Process – The Framework Functions and critical infrastructure risk management practices are formally supported by management and expressed as policy. The cybersecurity practices are regularly updated based on the application of risk management processes to a changing threat and technology landscape. o Integrated Program – There is a formalized approach to manage cybersecurity risk for the critical infrastructure operations. Repeatable, risk-informed policies, processes, and procedures are defined, implemented as intended, and validated. Consistent methods are in place to effectively respond to changes in risk. There are adequate personnel resource who possess the knowledge and skills to perform their appointed cybersecurity roles and responsibilities.

50	APPA-LPPC		T	11	358-371	2.4 Framework Implementation Tiers	The Tier 3 text has been modified to include the connection to the Framework Functions. This could also be said to be the Framework Core. The intent of this change is to create a tie to the Framework Profile creation process and a way for organizations to determine not only their Risk Management strategy but their institutionalization of the Framework Core to achieve greater cybersecurity.	o Information Sharing – Cybersecurity information is shared in a consistent documents process within the organization. The organization understands its critical infrastructure dependencies and partners and receives information from these partners enabling collaboration and risk-based management decisions within the organization in response to events.
51	APPA-LPPC		T	10	371-385	2.4 Framework Implementation Tiers	The Tier 4 text has been modified to include the connection to the Framework Functions. This could also be said to be the Framework Core. The intent of this change is to create a tie to the Framework Profile creation process and a way for organizations to determine not only their Risk Management strategy but their institutionalization of the Framework Core to achieve greater cybersecurity.	• Tier 4: Adaptive o Risk Management Process – The Framework Functions and critical infrastructure risk management practices are implemented in a manner that allows the organization to readily adapt its cybersecurity practices based on lessons learned and predictive indicators derived from previous cybersecurity activities. Through a process of continuous improvement, the organization actively adapts to a changing cybersecurity landscape and responds to emerging/evolving threats in a timely manner.

52	APPA-LPPC		T	11	371-386	2.4 Framework Implementation Tiers	The Tier 4 text has been modified to include the connection to the Framework Functions. This could also be said to be the Framework Core. The intent of this change is to create a tie to the Framework Profile creation process and a way for organizations to determine not only their Risk Management strategy but their institutionalization of the Framework Core to achieve greater cybersecurity.	o Integrated Program – There is an organization-wide approach to managing cybersecurity risk that uses risk-informed policies, processes, and procedures to address potential cybersecurity events. Cybersecurity risk management is part of the organizational culture and evolves from an awareness of previous activities, information shared by other sources, and continuous awareness of activities on their systems and networks that support critical infrastructure.
53	APPA-LPPC		T	12	371-387	2.4 Framework Implementation Tiers	The Tier 4 text has been modified to include the connection to the Framework Functions. This could also be said to be the Framework Core. The intent of this change is to create a tie to the Framework Profile creation process and a way for organizations to determine not only their Risk Management strategy but their institutionalization of the Framework Core to achieve greater cybersecurity.	o Information Sharing – The organization manages risk and actively shares information with internally and externally to ensure that accurate, current information is being distributed and consumed to improve the cybersecurity risk posture before an event occurs.

54	APPA-LPPC		E	10	386-389	2.4 Framework Implementation Tiers	This is helpful information to the selection process. This may be better suited as a callout box or footnote.	Move this text into the paragraph at the beginning of the section lines 322-331. This could be a call out box.
55	APPA-LPPC		T	9	332	2.4 Framework Implementation Tiers	This is alternative text for the Tier 0 definitions that pulls the Framework Functions out of the Risk Management Process definition and creates a separate Framework Functions (or Framework Core) definition.	• Tier 0: Not Initiated o Tier 1 has not been achieved.

56	APPA-LPPC		T	9	332-346	2.4 Framework Implementation Tiers	This is alternative text for the Tier 1 definitions that pulls the Framework Functions out of the Risk Management Process definition and creates a separate Framework Functions (or Framework Core) definition.	• Tier 1: Initiated o Framework Functions – The implementation of the Framework Functions are not formalized and may be ad hoc, irregular, and sometimes reactive to cybersecurity events. o Risk Management Process – The critical infrastructure cybersecurity risk management practices are not formalized and risk is managed in an ad hoc, irregular and sometimes reactive manner. Prioritization of cybersecurity activities may not be directly informed by organizational risk objectives, the threat environment, or critical infrastructure business/mission requirements. o Integrated Program – There is a limited awareness of cybersecurity risk at the organizational level. The organization implements cybersecurity risk management on an irregular, case-by-case basis due to varied experience or inadequate resources.
57	APPA-LPPC		T	10	332-347	2.4 Framework Implementation Tiers	This is alternative text for the Tier 1 definitions that pulls the Framework Functions out of the Risk Management Process definition and creates a separate Framework Functions (or Framework Core) definition.	o Information Sharing – The organization may not have processes that enable cybersecurity information to be shared within the organization. An organization may not have the processes in place to participate in coordination or collaboration with other entities.

58	APPA-LPPC		T	10	347-357	2.4 Framework Implementation Tiers	This is alternative text for the Tier 2 definitions that pulls the Framework Functions out of the Risk Management Process definition and creates a separate Framework Functions (or Framework Core) definition.	• Tier 2: Risk-Informed o Framework Functions – The implementation of the Framework Functions are approved by management, include limited information about cybersecurity risks, but may not be documented in policy. o Risk Management Process – The critical infrastructure risk management practices are approved by management but may not be established as documented policy. o Integrated Program – There is an awareness of cybersecurity risk at the critical infrastructure operations level but an integrated, overall organization-wide approach to managing critical infrastructure cybersecurity risk has not been established. Risk-informed processes and procedures are identified. Cybersecurity personnel resources have been identified but may not be dedicated to or have sufficient knowledge and skills to perform their cybersecurity duties.
59	APPA-LPPC		T	11	347-358	2.4 Framework Implementation Tiers	This is alternative text for the Tier 2 definitions that pulls the Framework Functions out of the Risk Management Process definition and creates a separate Framework Functions (or Framework Core) definition.	o Information Sharing – Cybersecurity information is shared within the organization on an informal basis. The organization knows its role in the larger critical infrastructure ecosystem, but has not formalized its capabilities to interact and share information externally.

60	APPA-LPPC		T	10	358-370	2.4 Framework Implementation Tiers	This is alternative text for the Tier3 definitions that pulls the Framework Functions out of the Risk Management Process definition and creates a separate Framework Functions (or Framework Core) definition.	• Tier 3: Repeatable o Framework Functions – The implementation of the Framework Functions are formally approved by management expressed in policy and receive adequate resources for sustainability. o Risk Management Process – The critical infrastructure risk management practices are formally approved by management and expressed as policy. The cybersecurity practices are regularly updated based on the application of risk management processes to a changing threat and technology landscape.
61	APPA-LPPC		T	11	358-371	2.4 Framework Implementation Tiers	This is alternative text for the Tier3 definitions that pulls the Framework Functions out of the Risk Management Process definition and creates a separate Framework Functions (or Framework Core) definition.	o Integrated Program – There is a formalized approach to manage cybersecurity risk for the critical infrastructure operations. Repeatable, risk-informed policies, processes, and procedures are defined, implemented as intended, and validated. Consistent methods are in place to effectively respond to changes in risk. There are adequate personnel resource who possess the knowledge and skills to perform their appointed cybersecurity roles and responsibilities.

62	APPA-LPPC		T	12	358-372	2.4 Framework Implementation Tiers	This is alternative text for the Tier3 definitions that pulls the Framework Functions out of the Risk Management Process definition and creates a separate Framework Functions (or Framework Core) definition.	o Information Sharing – Cybersecurity information is shared in a consistent documents process within the organization. The organization understands its dependencies and partners and receives information from these partners enabling collaboration and risk-based management decisions within the organization in response to events.

63	APPA-LPPC		T	10	371-385	2.4 Framework Implementation Tiers	This is alternative text for the Tier 4 definitions that pulls the Framework Functions out of the Risk Management Process definition and creates a separate Framework Functions (or Framework Core) definition.	• Tier 4: Adaptive o Framework Functions – The implementation of the Framework Functions are continuously monitored to ensure they are still meeting the intended cybersecurity risk management outcomes. o Risk Management Process – The critical infrastructure risk management practices are implemented in a manner that allows the organization to readily adapt its cybersecurity practices based on lessons learned and predictive indicators derived from previous cybersecurity activities. Through a process of continuous improvement, the organization actively adapts to a changing cybersecurity landscape and responds to emerging/evolving threats in a timely manner.

64	APPA-LPPC		T	11	371-386	2.4 Framework Implementation Tiers	This is alternative text for the Tier 4 definitions that pulls the Framework Functions out of the Risk Management Process definition and creates a separate Framework Functions (or Framework Core) definition.	o Integrated Program – There is an organization-wide approach to managing cybersecurity risk that uses risk-informed policies, processes, and procedures to address potential cybersecurity events. Cybersecurity risk management is part of the organizational culture and evolves from an awareness of previous activities, information shared by other sources, and continuous awareness of activities on their systems and networks.
65	APPA-LPPC		T	12	371-387	2.4 Framework Implementation Tiers	This is alternative text for the Tier 4 definitions that pulls the Framework Functions out of the Risk Management Process definition and creates a separate Framework Functions (or Framework Core) definition.	o Information Sharing – The organization manages risk and actively shares information with internally and externally to ensure that accurate, current information is being distributed and consumed to improve the cybersecurity risk posture before an event occurs.
66	APPA-LPPC		T		307-320	2.4 Framework Implementation Tiers	This text was moved to strengthen the Section 3 How To Use the Framework content.	The original text starting from line 307 and ending at line 320, including the graphic, is moved to line 408.
67	APPA-LPPC		T	11	396	3.0 How to use the Framework	Merge this section into one section. The steps would be useful for someone that is reviewing their existing program and for someone starting out	remove 3.1 Basic Overview of Cybersecurity Practices header

68	APPA-LPPC		T	11	391-395	3.0 How to use the Framework	Providing new rewording for the introduction	3.0 How to Use the Framework The Framework is designed to complement existing critical infrastructure cybersecurity operations or serve as the foundation for a new cybersecurity program. The Framework also provides a means of expressing cybersecurity requirements to business partners and customers and can help identify gaps and improvements to critical infrastructure cybersecurity practices. Using the Framework, organizations can examine what capabilities they have implemented in the five high-level Functions identified in the Framework Core.

69	APPA-LPPC		T	11	397-401	3.1 Basic Overview of Cybersecurity Practices	This section has been reworded into the introduction. There is a new Section 3.1 Coordination of Framework Implementation which came from Section 2.3	3.1 Coordination of Framework Implementation Figure 3 describes the notional flow of information and decisions within an organization: at the senior executive level, at the business/process level, and at the implementation/operations level. The critical infrastructure senior executive level communicates the mission priorities, available resources, and overall risk tolerance to the business/process level. The business/process level uses the information as inputs into their risk management process, and then collaborates with the implementation/operations level to create a Profile.

70	APPA-LPPC		T	12	397-402	3.1 Basic Overview of Cybersecurity Practices	This section has been reworded into the introduction. There is a new Section 3.1 Coordination of Framework Implementation which came from Section 2.4	The implementation/operation level communicates the Profile implementation to the business/process level. The business/process level uses this information to perform an impact assessment. The outcomes of that impact assessment are reported to the senior executive level to inform the organization's overall risk management process. Figure 3: Notional Information and Decision Flows within an Organization

71	APPA-LPPC		T	11	402-436	3.2 Using the Framework	Reworded the steps to create a close connection between the identification of Current Profile, the use of the Framework Core, a Target Profile and a continuous improvement cycle.	3.2 Using the Framework The following recursive steps illustrate how an organization could use the Framework Core, Profiles and Tiers to assess and update an existing cybersecurity program; or create a new cybersecurity program. The use of Profiles in this manner enables the organization to make informed decisions about cybersecurity activities, supports cost/benefit analysis, and enables the organization to create an action plan for targeted improvements.

72	APPA-LPPC		T	12	402-437	3.2 Using the Framework	Reworded the steps to create a close connection between the identification of Current Profile, the use of the Framework Core, a Target Profile and a continuous improvement cycle.	Step 1: The organization identifies the scope of the critical infrastructure operations that will be assessed in the Step 2 activity. The organization identifies relative to their critical infrastructure operations, systems and assets, the associated risk tolerances, threats, vulnerabilities, constraints, impacts of a cybersecurity event, voluntary and mandatory regulatory requirements and overall risk management approach. The organization also selects the appropriate Framework Informative References or chooses other Informative References that are sector or organization specific.

73	APPA-LPPC		T	13	402-438	3.2 Using the Framework	Reworded the steps to create a close connection between the identification of Current Profile, the use of the Framework Core, a Target Profile and a continuous improvement cycle.	Step 2: The organization develops a Current Framework Profile using each of the Framework Core Functions, Categories and Subcategories. The organization performs an assessment of their existing critical infrastructure cybersecurity practices according to the critical infrastructure operations that were selected in the Step 1 activity. Step 3: The organization analyzes the results of the Current Framework Profile to determine which Framework Tier corresponds to their existing critical infrastructure cybersecurity practices. The organization then determines whether the existing "Current State" Framework Profile is sufficient based on the risk management approach identified in the Step 1 activity.

74	APPA-LPPC		T	14	402-439	3.2 Using the Framework	Reworded the steps to create a close connection between the identification of Current Profile, the use of the Framework Core, a Target Profile and a continuous improvement cycle.	Step 4: If the organization desires modify its Current Framework Profile, the organization can create a Target Framework Profile that focuses on determining the desired cybersecurity outcome along with a desired Framework Tier. The organization develops and implements an action plan to deploy the cybersecurity practices in the "Target State" Framework Profile. Step 5: Once the organization achieves the Target Framework Profile, it then implements a monitoring plan to ensure selected cybersecurity practices are achieving the desired outcomes over time. The organization also develops a continuous monitoring strategy for when to initiate the recursive Step 1 activity.
75	APPA-LPPC		T	13-25		Appendix A: Framework Core	Include NERC CIP Standards as informative References throughout the Framework Core	Add the NERC CIP Standards Mapping developed by DOE and NERC to each category and subcategory. http://www.nerc.com/pa/Stand/Pages/AllReliabilityStandards.aspx?jurisdiction=United States
76	APPA-LPPC		T	13	457	Appendix A	The Appendix A is the Framework Core and should be considered a section within the Framework document. The main document content is critical to the implementation of the Appendix A.	Rename to Section 4: Framework Core

77	APPA-LPPC		T	13	459	Appendix A		change "activities" to "outcomes"
78	APPA-LPPC		T	13	460	Appendix A	This statement is confusing. The next statement says that it is extensible. The Framework Core as presented is the baseline. It is possible to add categories and subcategories through the Profile process, but nothing should be removed.	remove "is not exhaustive"
79	APPA-LPPC		T	13		Asset Management (AM)	Rewording the categories and subcategories to relate directly to critical infrastructure and to provide consistent language and flow throughout each of the Functions.	The critical infrastructure personnel, devices, systems, facilities and information are identified and managed consistent with their relative importance to risk management practices.
80	APPA-LPPC		T				Systems, software, hardware, data flows, etc. are all identified, but there is no data classification in this Function.	Add a subcategory: For critical infrastructure, the data and information is classified and labeled
81	APPA-LPPC		T	13		ID.AM-1	Rewording the categories and subcategories to relate directly to critical infrastructure and to provide consistent language and flow throughout each of the Functions.	For critical infrastructure, the physical assets and systems are inventoried

82	APPA-LPPC		T	13		ID.AM-2	Rewording the categories and subcategories to relate directly to critical infrastructure and to provide consistent language and flow throughout each of the Functions.	For critical infrastructure, the software platforms and applications are inventoried
83	APPA-LPPC		T	13		ID.AM-3	Rewording the categories and subcategories to relate directly to critical infrastructure and to provide consistent language and flow throughout each of the Functions.	For critical infrastructure, the communication data flows are mapped
84	APPA-LPPC		T	14		ID.AM-4	Rewording the categories and subcategories to relate directly to critical infrastructure and to provide consistent language and flow throughout each of the Functions.	For critical infrastructure, the internal and external system interfaces are identified documented and mapped
85	APPA-LPPC		T	14		ID.AM-5	Rewording the categories and subcategories to relate directly to critical infrastructure and to provide consistent language and flow throughout each of the Functions.	For critical infrastructure, the personnel resources are prioritized …

86	APPA-LPPC		T	14		ID.AM-6	Rewording the categories and subcategories to relate directly to critical infrastructure and to provide consistent language and flow throughout each of the Functions.	For critical infrastructure, the personnel roles and responsibilities for cybersecurity in IT and ICS are identified, documented, communicated and managed
87	APPA-LPPC		T	14		Business Environment (BE)	Rewording the categories and subcategories to relate directly to critical infrastructure and to provide consistent language and flow throughout each of the Functions.	For critical infrastructure, the mission, objectives….
88	APPA-LPPC		T	14		ID.BE-1	Rewording the categories and subcategories to relate directly to critical infrastructure and to provide consistent language and flow throughout each of the Functions.	For critical infrastructure, the supply chain cybersecurity requirements are identified and communicated
89	APPA-LPPC		T	14		ID.BE-2	Rewording the categories and subcategories to relate directly to critical infrastructure and to provide consistent language and flow throughout each of the Functions.	For critical infrastructure, the role in their industry ecosystem is identified, documented and communicated

90	APPA-LPPC		T	14		ID.BE-3	Rewording the categories and subcategories to relate directly to critical infrastructure and to provide consistent language and flow throughout each of the Functions.	For critical infrastructure, the mission and business objectives and activities are identified, documented, prioritized and communicated
91	APPA-LPPC		T	14		ID.BE-4	Rewording the categories and subcategories to relate directly to critical infrastructure and to provide consistent language and flow throughout each of the Functions.	For critical infrastructure, the internal and external dependencies are identified, documented and communicated
92	APPA-LPPC		T	15		ID.BE-5	Rewording the categories and subcategories to relate directly to critical infrastructure and to provide consistent language and flow throughout each of the Functions.	For critical infrastructure, the resiliency requirements are identified, documented, prioritized and communicated
93	APPA-LPPC		T	15		Governance (GV)	Rewording the categories and subcategories to relate directly to critical infrastructure and to provide consistent language and flow throughout each of the Functions.	For critical infrastructure, the policies, procedures and processes to manage and monitor the regulatory, legal, risk, environmental and operational requirements are understood and inform the management of cybersecurity risk.

94	APPA-LPPC		T	15		ID.GV-1	Rewording the categories and subcategories to relate directly to critical infrastructure and to provide consistent language and flow throughout each of the Functions.	For critical infrastructure, the cybersecurity policy(is) are identified, documented and communicated
95	APPA-LPPC		T	15		ID.GV-2	Rewording the categories and subcategories to relate directly to critical infrastructure and to provide consistent language and flow throughout each of the Functions.	For critical infrastructure, the cybersecurity roles and responsibilities are established and communicated
96	APPA-LPPC		T	15		ID.GV-3	Rewording the categories and subcategories to relate directly to critical infrastructure and to provide consistent language and flow throughout each of the Functions.	For critical infrastructure, the legal and regulatory requirements for cybersecurity, including privacy and civil liberties obligations, are identified, documented and communicated
97	APPA-LPPC		T	15		ID.GV-4	Rewording the categories and subcategories to relate directly to critical infrastructure and to provide consistent language and flow throughout each of the Functions.	For critical infrastructure, the governance model includes cybersecurity practices

98	APPA-LPPC		T	15		Risk Assessment (RA)	Rewording the categories and subcategories to relate directly to critical infrastructure and to provide consistent language and flow throughout each of the Functions.	For critical infrastructure, the cybersecurity risk to operations, including mission and business, image and reputation, assets and individuals is documented
99	APPA-LPPC		T	15		ID.RA-1	Rewording the categories and subcategories to relate directly to critical infrastructure and to provide consistent language and flow throughout each of the Functions.	For critical infrastructure, the asset vulnerabilities are identified, documented and prioritized for risk response and integrated into the cybersecurity program
100	APPA-LPPC		T	15		ID.RA-2	Rewording the categories and subcategories to relate directly to critical infrastructure and to provide consistent language and flow throughout each of the Functions.	For critical infrastructure, the threat and vulnerability information is received from information sharing forums and sources and integrated into the cybersecurity program
101	APPA-LPPC		T	16		ID.RA-3	Rewording the categories and subcategories to relate directly to critical infrastructure and to provide consistent language and flow throughout each of the Functions.	For critical infrastructure, the threats to assets are identified, documented, prioritized for risk response and integrated into the cybersecurity program

102	APPA-LPPC		T	16		ID.RA-4	Rewording the categories and subcategories to relate directly to critical infrastructure and to provide consistent language and flow throughout each of the Functions.	For critical infrastructure, the threat and vulnerability impacts are identified, documented, prioritized for risk response and integrated into the cybersecurity program
103	APPA-LPPC		T	16		ID.RA-5	Rewording the categories and subcategories to relate directly to critical infrastructure and to provide consistent language and flow throughout each of the Functions.	For critical infrastructure, the cybersecurity threat and vulnerability risk responses are identified, documented, prioritized for risk response and integrated into the cybersecurity program
104	APPA-LPPC		T	16		Risk Management Strategy (RM)	Rewording the categories and subcategories to relate directly to critical infrastructure and to provide consistent language and flow throughout each of the Functions.	The critical infrastructure cybersecurity risk management strategy is established and includes priorities, constraints, risk tolerances, and assumptions to support cybersecurity risk decisions
105	APPA-LPPC		T	16		ID.RM-1	Rewording the categories and subcategories to relate directly to critical infrastructure and to provide consistent language and flow throughout each of the Functions.	For critical infrastructure, the cybersecurity risk management processes are identified, documented, prioritized for risk response, and integrated into the cybersecurity program

106	APPA-LPPC		T	16		ID.RM-2	Rewording the categories and subcategories to relate directly to critical infrastructure and to provide consistent language and flow throughout each of the Functions.	For critical infrastructure, the cybersecurity risk tolerances are identified, documented, prioritized for risk response, and integrated into the cybersecurity program.
107	APPA-LPPC		T	16		ID.RM-3	Rewording the categories and subcategories to relate directly to critical infrastructure and to provide consistent language and flow throughout each of the Functions.	For critical infrastructure, the determination of risk tolerance is informed by the role in their industry and any sector specific risk analysis
108	APPA-LPPC		T	16		Access Control (AC)	Rewording the categories and subcategories to relate directly to critical infrastructure and to provide consistent language and flow throughout each of the Functions.	The critical infrastructure accesses to associated information resources and facilities are limited to authorized people processes, systems, and activities.
109	APPA-LPPC		T	16		PR.AC-1	Rewording the categories and subcategories to relate directly to critical infrastructure and to provide consistent language and flow throughout each of the Functions.	For critical infrastructure, the identities and credentials for systems and people is identified, documented and managed.

110	APPA-LPPC		T	17		PR.AC-2	Rewording the categories and subcategories to relate directly to critical infrastructure and to provide consistent language and flow throughout each of the Functions.	For critical infrastructure, the physical access is identified, documented and managed.
111	APPA-LPPC		T	17		PR.AC-3	Rewording the categories and subcategories to relate directly to critical infrastructure and to provide consistent language and flow throughout each of the Functions.	For critical infrastructure, the remote access to systems is identified, documented, and managed.
112	APPA-LPPC		T	17		PR-AC-4	Rewording the categories and subcategories to relate directly to critical infrastructure and to provide consistent language and flow throughout each of the Functions.	For critical infrastructure, the access permissions to systems is identified, documented, and managed
113	APPA-LPPC		T	17		PR-AC-5	Rewording the categories and subcategories to relate directly to critical infrastructure and to provide consistent language and flow throughout each of the Functions.	For critical infrastructure, the processes for maintaining network integrity is identified, documented, and managed

114	APPA-LPPC		T	17		Awareness and Training (AT)	Rewording the categories and subcategories to relate directly to critical infrastructure and to provide consistent language and flow throughout each of the Functions.	The critical infrastructure personnel and partners are adequately trained to perform their cybersecurity related duties and responsibilities consistent with established policies, procedures and agreements.
115	APPA-LPPC		T	17		PR.AT-1	Rewording the categories and subcategories to relate directly to critical infrastructure and to provide consistent language and flow throughout each of the Functions.	For critical infrastructure, the people accessing facilities and systems are informed and trained on their cybersecurity responsibilities
116	APPA-LPPC		T	17		PR.AT-2	Rewording the categories and subcategories to relate directly to critical infrastructure and to provide consistent language and flow throughout each of the Functions.	For critical infrastructure, the privileged users are informed and trained on their cybersecurity responsibilities
117	APPA-LPPC		T	18		PR.AT-3	Rewording the categories and subcategories to relate directly to critical infrastructure and to provide consistent language and flow throughout each of the Functions.	For critical infrastructure, the third-party stakeholders, including customers and partners are informed and trained on their cybersecurity responsibilities

118	APPA-LPPC		T	18		PR.AT-4	Rewording the categories and subcategories to relate directly to critical infrastructure and to provide consistent language and flow throughout each of the Functions.	For critical infrastructure, the senior executives are informed and trained on their cyber security responsibilities
119	APPA-LPPC		T	18		PR.AT-5	Rewording the categories and subcategories to relate directly to critical infrastructure and to provide consistent language and flow throughout each of the Functions.	For critical infrastructure, the physical security and cybersecurity personnel are informed and trained on their cybersecurity responsibilities
120	APPA-LPPC		T	18		Data Security (DS)	Rewording the categories and subcategories to relate directly to critical infrastructure and to provide consistent language and flow throughout each of the Functions.	The critical infrastructure records and data are managed consistent with the organization's risk management strategy to protect the confidentiality, integrity and availability.
121	APPA-LPPC		T	18		PR.DS-1	Rewording the categories and subcategories to relate directly to critical infrastructure and to provide consistent language and flow throughout each of the Functions.	For critical infrastructure, the data at rest is protected based on the risk management strategy

122	APPA-LPPC		T	18		PR.DS-2	Rewording the categories and subcategories to relate directly to critical infrastructure and to provide consistent language and flow throughout each of the Functions.	For critical infrastructure, the data in motion is protected based on the risk management strategy
123	APPA-LPPC		T	18		PR.DS-3	Rewording the categories and subcategories to relate directly to critical infrastructure and to provide consistent language and flow throughout each of the Functions.	For critical infrastructure, the assets are managed throughout their entire lifecycle of acquisition, implementation, redeployment and destruction is protected based on the risk management strategy
124	APPA-LPPC		T	19		PR.DS-4	Rewording the categories and subcategories to relate directly to critical infrastructure and to provide consistent language and flow throughout each of the Functions.	For critical infrastructure, the availability requirements are identified, documented and managed based on the risk management strategy
125	APPA-LPPC		T	19		PR.DS-5	Rewording the categories and subcategories to relate directly to critical infrastructure and to provide consistent language and flow throughout each of the Functions.	For critical infrastructure, the protections against data leakage of confidential information are identified, documented and managed based on the risk management strategy

126	APPA-LPPC		T	19		PR.DS-6	Covered in PR.DS-5	Remove this requirement.
127	APPA-LPPC		T	19		PR.DS-7	Covered in PR.DS-3	Remove this requirement.
128	APPA-LPPC		T	19		PR.DS-8	Rewording the categories and subcategories to relate directly to critical infrastructure and to provide consistent language and flow throughout each of the Functions.	For critical infrastructure, the development and testing environments are separated from production based on the risk management strategy
129	APPA-LPPC		T	19		PR.PDS-9	Rewording the categories and subcategories to relate directly to critical infrastructure and to provide consistent language and flow throughout each of the Functions.	For critical infrastructure, the privacy of individuals and personally identifiable information (PII) is protected based on the risk management strategy
130	APPA-LPPC		T	19		Information Protection Processes and Procedures (IP)	Rewording the categories and subcategories to relate directly to critical infrastructure and to provide consistent language and flow throughout each of the Functions.	The critical infrastructure cybersecurity policy addresses the purpose, scope, roles, responsibilities, management commitment and coordination; processes and procedures are maintained and used to manage the protection of critical infrastructure systems.

131	APPA-LPPC		T	19		PR.IP-1	Rewording the categories and subcategories to relate directly to critical infrastructure and to provide consistent language and flow throughout each of the Functions.	For critical infrastructure, the configuration management baseline is identified, documented and managed
132	APPA-LPPC		T	19		PR.IP-2	Rewording the categories and subcategories to relate directly to critical infrastructure and to provide consistent language and flow throughout each of the Functions.	For critical infrastructure, the Systems Development Lifecycle is identified, documented and managed
133	APPA-LPPC		T	20		PR.IP-3	Rewording the categories and subcategories to relate directly to critical infrastructure and to provide consistent language and flow throughout each of the Functions.	For critical infrastructure, the configuration management and change control processes are identified, documented and managed
134	APPA-LPPC		T	20		PR-IP-4	Rewording the categories and subcategories to relate directly to critical infrastructure and to provide consistent language and flow throughout each of the Functions.	For critical infrastructure, the system backups are identified, documented and managed

135	APPA-LPPC		T	20		PR.IP-5	Rewording the categories and subcategories to relate directly to critical infrastructure and to provide consistent language and flow throughout each of the Functions.	what does this one mean?
136	APPA-LPPC		T	20		PR.IP-6	Rewording the categories and subcategories to relate directly to critical infrastructure and to provide consistent language and flow throughout each of the Functions.	For critical infrastructure, the confidential information is destroyed according to documented policies and procedures
137	APPA-LPPC		T	20		PR.IP-7	Rewording the categories and subcategories to relate directly to critical infrastructure and to provide consistent language and flow throughout each of the Functions.	For critical infrastructure, the policies and procedures that support the Information Protection Processes and Procedures are continuously approved according to the cybersecurity risk management strategy
138	APPA-LPPC		T	20		PR.IP-8	Rewording the categories and subcategories to relate directly to critical infrastructure and to provide consistent language and flow throughout each of the Functions.	For critical infrastructure, the sharing of relevant threat and vulnerability information occurs with appropriate parties

139	APPA-LPPC		T	20		PR.IP-9	Rewording the categories and subcategories to relate directly to critical infrastructure and to provide consistent language and flow throughout each of the Functions.	For critical infrastructure, the Response Plans, Business Continuity Plans, Disaster Recovery Plans, and Incident Handling Plans are identified, documented, communicated and managed
140	APPA-LPPC		T	21		PR.IP-10	Rewording the categories and subcategories to relate directly to critical infrastructure and to provide consistent language and flow throughout each of the Functions.	For critical infrastructure, the Plans identified in PR.IP-9 are exercised according to the cybersecurity risk management strategy
141	APPA-LPPC		T	21		PR.IP-11	Rewording the categories and subcategories to relate directly to critical infrastructure and to provide consistent language and flow throughout each of the Functions.	For critical infrastructure, the human resources practices for on-boarding, off-boarding, privilege management are identified, documented and managed
142	APPA-LPPC		T	21		Maintenance (MA)	Rewording the categories and subcategories to relate directly to critical infrastructure and to provide consistent language and flow throughout each of the Functions.	The critical infrastructure practices for the maintenance and repair of system components is performed consistent with identified, documented and communicated policies and procedures

143	APPA-LPPC		T	21		PR.MA-1	Rewording the categories and subcategories to relate directly to critical infrastructure and to provide consistent language and flow throughout each of the Functions.	For critical infrastructure, the maintenance and repair of assets is documented and approved
144	APPA-LPPC		T	21		PR.MA-2	Rewording the categories and subcategories to relate directly to critical infrastructure and to provide consistent language and flow throughout each of the Functions.	For critical infrastructure, the remote maintenance is performed consistent with PR.AC-3
145	APPA-LPPC		T	21		Protective Technology (PT)	Rewording the categories and subcategories to relate directly to critical infrastructure and to provide consistent language and flow throughout each of the Functions.	The critical infrastructure technical security solutions are managed to ensure the security and resilience of systems and assets, consistent with related policies, procedures, and agreements.
146	APPA-LPPC		T	21		PR.PT-1	Rewording the categories and subcategories to relate directly to critical infrastructure and to provide consistent language and flow throughout each of the Functions.	For critical infrastructure, the audit log retention requirements are identified and documented to support the Detect and Respond Functions and in accordance with the cybersecurity risk management strategy

147	APPA-LPPC		T	21		PR.PT-2	Rewording the categories and subcategories to relate directly to critical infrastructure and to provide consistent language and flow throughout each of the Functions.	For critical infrastructure, the physical and logical ports of assets are managed according to the cybersecurity risk management strategy
148	APPA-LPPC		T	21		PR.PT-3	Rewording the categories and subcategories to relate directly to critical infrastructure and to provide consistent language and flow throughout each of the Functions.	For critical infrastructure, the physical and logical access to assets are managed according to the cybersecurity risk management strategy
149	APPA-LPPC		T	21		PR.PT-4	Rewording the categories and subcategories to relate directly to critical infrastructure and to provide consistent language and flow throughout each of the Functions.	For critical infrastructure, the communication network connections are secured according to the cybersecurity risk management strategy
150	APPA-LPPC		T	22		Anomalies and Events (AE)	Rewording the categories and subcategories to relate directly to critical infrastructure and to provide consistent language and flow throughout each of the Functions.	The critical infrastructure potential impacts associated with anomalous communication is detected in a timely manner to support the Respond Function

151	APPA-LPPC		T	22		DE.AE-2	This requirement does not appear to be different from ID.AM-3.	Remove this requirement.
152	APPA-LPPC		T	22		DE.AE-2	Rewording the categories and subcategories to relate directly to critical infrastructure and to provide consistent language and flow throughout each of the Functions.	For critical infrastructure, the detected cybersecurity events are analyzed to understand attack targets and methods
153	APPA-LPPC		T	22		DE.AE-3	Wonder if this should tie back to ISAC?	For critical infrastructure, the data associated with cybersecurity events is correlated from diverse information sources
154	APPA-LPPC		T	22		DE.AE-4	Rewording the categories and subcategories to relate directly to critical infrastructure and to provide consistent language and flow throughout each of the Functions.	For critical infrastructure, the detected cybersecurity events are analyzed to determine their impacts

155	APPA-LPPC		T	22		DE.AE-5	Rewording the categories and subcategories to relate directly to critical infrastructure and to provide consistent language and flow throughout each of the Functions.	For critical infrastructure, the alerts to support incident handling and the Respond Function are identified, documented and managed according to the cybersecurity risk management strategy
156	APPA-LPPC		T	22		Security Continuous Monitoring (CM)	Rewording the categories and subcategories to relate directly to critical infrastructure and to provide consistent language and flow throughout each of the Functions.	The critical infrastructure assets are continuously monitored to identify cybersecurity events and to verify the effectiveness of the Protect Function measures.
157	APPA-LPPC		T	22		DE.CM-1	Rewording the categories and subcategories to relate directly to critical infrastructure and to provide consistent language and flow throughout each of the Functions.	For critical infrastructure, the communication networks are continuously monitored to detect potential cybersecurity events according to the cybersecurity risk management strategy

158	APPA-LPPC		T	22		DE.CM-2	Rewording the categories and subcategories to relate directly to critical infrastructure and to provide consistent language and flow throughout each of the Functions.	For critical infrastructure, the physical environment is continuously monitored to detect potential cyber-physical events according to the cybersecurity risk management strategy
159	APPA-LPPC		T	22		DE.CM-3	Rewording the categories and subcategories to relate directly to critical infrastructure and to provide consistent language and flow throughout each of the Functions.	For critical infrastructure, the personnel activity is continuously monitored to detect potential cybersecurity events according to the risk management strategy
160	APPA-LPPC		T	22		DE.CM-4	Rewording the categories and subcategories to relate directly to critical infrastructure and to provide consistent language and flow throughout each of the Functions.	For critical infrastructure, the methods to detect malicious code are identified, documented and managed

161	APPA-LPPC		T	23		DE.CM-5	Rewording the categories and subcategories to relate directly to critical infrastructure and to provide consistent language and flow throughout each of the Functions.	For critical infrastructure, the methods to detect mobile code are identified, documented and managed
162	APPA-LPPC		T	23		DE.CM-6	Rewording the categories and subcategories to relate directly to critical infrastructure and to provide consistent language and flow throughout each of the Functions.	critical infrastructure, the methods to monitor external service providers are identified, documented and managed
163	APPA-LPPC		T	23		DE.CM-7	Rewording the categories and subcategories to relate directly to critical infrastructure and to provide consistent language and flow throughout each of the Functions.	NOT SURE WHAT RESOURCES THIS REFERS TO? - application processes? People?

164	APPA-LPPC		T	23		DE.CM-8	Rewording the categories and subcategories to relate directly to critical infrastructure and to provide consistent language and flow throughout each of the Functions.	For critical infrastructure, the cybersecurity vulnerability assessments are performed according to the cybersecurity risk management strategy
165	APPA-LPPC		T	23		Detection Processes (DP)	Rewording the categories and subcategories to relate directly to critical infrastructure and to provide consistent language and flow throughout each of the Functions.	The critical infrastructure detection processes and procedures are maintained and tested to ensure timely and adequate awareness of anomalous events
166	APPA-LPPC		T	23		DE.DP-1	Rewording the categories and subcategories to relate directly to critical infrastructure and to provide consistent language and flow throughout each of the Functions.	For critical infrastructure, the cybersecurity personnel roles and responsibilities for detection are identified, documented, communicated and managed

167	APPA-LPPC		T	23		DE.DP-2	Rewording the categories and subcategories to relate directly to critical infrastructure and to provide consistent language and flow throughout each of the Functions.	For critical infrastructure, the detection activities comply with legal, regulatory, privacy and civil liberties requirements
168	APPA-LPPC		T	23		DE.DP-3	Rewording the categories and subcategories to relate directly to critical infrastructure and to provide consistent language and flow throughout each of the Functions.	For critical infrastructure, the detection activities are identified, documented, exercised and managed
169	APPA-LPPC		T	23		DE.DP-4	Rewording the categories and subcategories to relate directly to critical infrastructure and to provide consistent language and flow throughout each of the Functions.	For critical infrastructure, the detected cybersecurity event information is communicated as part of identified and documented information sharing practices

170	APPA-LPPC		T	23		DE.DP-5	Rewording the categories and subcategories to relate directly to critical infrastructure and to provide consistent language and flow throughout each of the Functions.	For critical infrastructure, the detection processes are continuously improved according to the cybersecurity risk management strategy
171	APPA-LPPC		T	24		Response Plan (RP)	Removed "and tested" because PR.IP-10 did the exercising of the Plans. Also change the name of the Category to "Response Plan" since the "planning" actually also occurred in the Protect Function.	The critical infrastructure response processes and procedures are implemented to ensure timely response of detected cybersecurity events
172	APPA-LPPC		T	24		RS.RP-1	Rewording the categories and subcategories to relate directly to critical infrastructure and to provide consistent language and flow throughout each of the Functions.	For critical infrastructure, the Response Plans maintained in PR.IP-10 are implemented during or after a detected cybersecurity event

173	APPA-LPPC		T	24		Communications (CO)	Rewording the categories and subcategories to relate directly to critical infrastructure and to provide consistent language and flow throughout each of the Functions.	The critical infrastructure response activities are coordinated with internal and external stakeholders to include external support from federal, state and local law enforcement
174	APPA-LPPC		T	24		RS.CO-1	Rewording the categories and subcategories to relate directly to critical infrastructure and to provide consistent language and flow throughout each of the Functions.	For critical infrastructure, the personnel roles and responsibilities for reporting cybersecurity events are identified, documented, communicated and managed
175	APPA-LPPC		T	24		RS.CO-2	Rewording the categories and subcategories to relate directly to critical infrastructure and to provide consistent language and flow throughout each of the Functions.	For critical infrastructure, the requirements for reporting detected cybersecurity events are identified, documented, communicated and managed

176	APPA-LPPC		T	24		RS.CO-3	Rewording the categories and subcategories to relate directly to critical infrastructure and to provide consistent language and flow throughout each of the Functions.	For critical infrastructure, the cybersecurity, privacy and civil liberties detection, response, and breach reporting requirements are identified, documented, communicated and managed according to the Response Plans created in PR.IP-10
177	APPA-LPPC		T	24		RS.CO-4	Rewording the categories and subcategories to relate directly to critical infrastructure and to provide consistent language and flow throughout each of the Functions.	For critical infrastructure, the coordination with internal and external stakeholders (e.g. business partners, information sharing and analysis centers, government entities) includes cybersecurity, privacy and civil liberties considerations in accordance with Response Plans created in PR.IP-10
178	APPA-LPPC		T	24		RS.CO-5	Included this language in RS.CO-4	Remove this requirement.

179	APPA-LPPC		T	24		Analysis (AN)	Rewording the categories and subcategories to relate directly to critical infrastructure and to provide consistent language and flow throughout each of the Functions.	The critical infrastructure establishes regular analysis of cybersecurity detection capabilities to support the Response and Recovery Functions.
180	APPA-LPPC		T	24		RS.AN-1	Rewording the categories and subcategories to relate directly to critical infrastructure and to provide consistent language and flow throughout each of the Functions.	For critical infrastructure, the alerts and notifications from cybersecurity detection systems are investigated according to the risk management strategy
181	APPA-LPPC		T	24		RS.AN-2	Rewording the categories and subcategories to relate directly to critical infrastructure and to provide consistent language and flow throughout each of the Functions.	For critical infrastructure, the impacts of a cybersecurity incident are analyzed, documented and communicated

182	APPA-LPPC		T	24		RS.AN-3	Rewording the categories and subcategories to relate directly to critical infrastructure and to provide consistent language and flow throughout each of the Functions.	For critical infrastructure, the analysis of evidence associated with a cybersecurity incident includes internal or external forensic analysis according to the cybersecurity risk management strategy
183	APPA-LPPC		T	25		RS.AN-4	Rewording the categories and subcategories to relate directly to critical infrastructure and to provide consistent language and flow throughout each of the Functions.	For critical infrastructure, the cybersecurity incidents are classified consistent with the Response Plans created in PR.IP-10
184	APPA-LPPC		T	25		Mitigation (MI)	Rewording the categories and subcategories to relate directly to critical infrastructure and to provide consistent language and flow throughout each of the Functions.	The critical infrastructure activities for mitigating a Cybesecurity incident are performed to prevent expansion of an event, mitigate its effects and eradicate the incident

185	APPA-LPPC		T	25		RS.MI-1	Possibly this should be a requirement in the PR.IP-10 as an element of the Response Plans or in the RP category of Response?	For critical infrastructure, the Response Plans are implemented to contain the expansion of a cybersecurity incident
186	APPA-LPPC		T	25		RS.MI-2	Possibly this should be a requirement in the PR.IP-10 as an element of the Response Plans or in the RP category of Response?	For critical infrastructure, the Response Plans are implemented to eradicate expansion and exposure of a cybersecurity incident
187	APPA-LPPC		T	25		Improvements (IM)	Rewording the categories and subcategories to relate directly to critical infrastructure and to provide consistent language and flow throughout each of the Functions.	The critical infrastructure response activities are improved by incorporating lessons learned from exercising the Response Plans or from actual detected cybersecurity incidents

188	APPA-LPPC		T	25		RS.IM-1	Rewording the categories and subcategories to relate directly to critical infrastructure and to provide consistent language and flow throughout each of the Functions.	For critical infrastructure, the Response Plans from PR.IP-10 incorporate lessons learned from exercising the Response Plans or from actual detected cybersecurity incidents
189	APPA-LPPC		T	25		RS.IM-2	Rewording the categories and subcategories to relate directly to critical infrastructure and to provide consistent language and flow throughout each of the Functions.	For critical infrastructure, the Response plans from PR.IP-10 are updated from exercising the Response Plans or from actual detected cybersecurity incidents
190	APPA-LPPC		T	25		Recovery Plan (RP)	Removed "tested" because PR.IP-10 did the exercising of the Plans. Also change the name of the Category to "Response Plan" since the "planning" actually also occurred in the Protect Function.	The critical infrastructure recovery processes and procedures are implemented to ensure timely response of detected cybersecurity events

191	APPA-LPPC		T	25		RC.RP-1	Rewording the categories and subcategories to relate directly to critical infrastructure and to provide consistent language and flow throughout each of the Functions.	For critical infrastructure, the Recovery Plans maintained in PR.IP-10 are implemented during or after a detected cybersecurity event
192	APPA-LPPC		T	25		Improvements (IM)	Rewording the categories and subcategories to relate directly to critical infrastructure and to provide consistent language and flow throughout each of the Functions.	The critical infrastructure recovery activities are improved by incorporating lessons learned from exercising the Response Plans or from actual detected cybersecurity incidents
193	APPA-LPPC		T	25		RC.IM-1	Rewording the categories and subcategories to relate directly to critical infrastructure and to provide consistent language and flow throughout each of the Functions.	For critical infrastructure, the Recovery Plans from PR.IP-10 incorporate lessons learned from exercising the Response Plans or from actual detected cybersecurity incidents

194	APPA-LPPC		T	25		RC.IM-2	Rewording the categories and subcategories to relate directly to critical infrastructure and to provide consistent language and flow throughout each of the Functions.	For critical infrastructure, the Response plans from PR.IP-10 are updated from exercising the Response Plans or from actual detected cybersecurity incidents
195	APPA-LPPC		T	25		Communications (CO)	Rewording the categories and subcategories to relate directly to critical infrastructure and to provide consistent language and flow throughout each of the Functions.	The critical infrastructure recovery activities are coordinated with internal and external stakeholders to include external support from federal, state and local law enforcement, information sharing and analysis centers, CSIRTs, vendors, etc.
196	APPA-LPPC		T	25		RC.CO-1	Rewording the categories and subcategories to relate directly to critical infrastructure and to provide consistent language and flow throughout each of the Functions.	For critical infrastructure, the requirements for managing public relations and reputation are identified, documented, communicated and managed

Type: E - Editorial, G - General T - Technical

197	APPA-LPPC		T	25		RC.CO-2	Integrated this requirements into RC.CO-1. Public Relations includes reputation management	Remove this requirement.
198	APPA-LPPC		T	27	478-484		This text and graphic is a great introduction to the Framework Core. It would help to acclimate the reader to the details that appear once they arrive at the Framework Core section	Move these lines to 395 - into the Section 3.0 How to Use the Framework
199	APPA-LPPC		T	36	497		Unclear how these areas became high priority, suggest that they are more potential areas for improvement that have been listed and described.	delete "high-priority," replace with "potential"
200	APPA-LPPC		T	36	498		How these were "identified" is unclear, suggest edits to be consistent with these areas are a discussion starting point, more work needs to be done.	replace "currently identified" with "listed and discussed below."

201	APPA-LPPC		E	36	498			change "These initial" to "The following"
202	APPA-LPPC		T	36	498	Appendix C	A list and description is not really a roadmap, but a starting point for discussion.	change "roadmap" to "discussion starting point"
203	APPA-LPPC		T	36	509-516	Appendix C	This discussion is premature, the existing framework needs to be tested first, then a more informed process to develop areas for improvement should come out of the Sector-Specific Agencies through the Sector Coordinating Councils	delete "but these highlighted…addressing the challenges."
204	APPA-LPPC		T	36	518-522	Appendix C	Prescriptive discussion, should be sector-specific and not in the NIST Framework.	delete "As a result, …such as a biometric."
205	APPA-LPPC		T	38	576-584	Appendix C	This is not an exhaustive list, sector-specific efforts are underway that are not included here, which can be confusing to the reader, lines 568-574 are adequate to address the area.	delete lines 576-584
206	APPA-LPPC		T	39	617-626	Appendix C	A detailed description of the shortcomings of the FIPPs is unclear here. This is to focus on the gap.	delete "Although the FIPPs…Privacy Methodology is limited." add "However, the FIPPs do not provide best practices and metrics for implementing privacy protections." delete "lack of standardization, and supporting privacy metrics,"

