Comments template for Preliminary
Cybersecurity Framework

Submitted by: ________________________
Date: ________________________

#	Organization	Commentor	Type	Page #	Line #	Section	Comment (Include rationale for comment)	Suggested change
1	UTC		ge			throughout	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. Furthermore, the use of the terms "organization" and "system" in the current Framework document is quite broad and not well defined. It is	Provide definitions of "organization" and "system" upfront in the document as follows: "Organization is a critical infrastructure owner/operator inclusive of the supporting supply chains." "System includes ICT and ICS assets that support operations of critical infrastructure." Review the use of the business terms such as "organization," "mission," and "business" for potential replacement with "critical infrastructure."
2	UTC		ge			throughout	The terms activities and outcomes are used interchangeably throughout the document. The intent of the Framework is that critical infrastructure owners and operators are going to achieve 'outcomes' associated with the	Change 'activities' to 'outcomes' throughout the document
3	UTC		te	1	71-76	1	In Note to Reviewers NIST asks "does the Preliminary Framework provide the tools for senior executives and boards of directors to iunderstand risks and mitigations….?" In our view, the Framework assumes understanding by the reader that critical infrastructure relies on IT and therefore cyber risks are important. We believe these are intuitive connections that need to be made explicit.	Expand the paragraph to explicitly state that: - Critical infrastructure relies on information technology for core functions - Technology is complex and can be vulnerable and therefore subject to risk - Threats are such that numerous parties can easily penetrate the technology and therefore do harm to the critical infrastructure
4	UTC		te	1	80-81	1	The sentence that starts from "To manage cybersecurity risks,…… is too general and detracts from the focus on critical infrastructure.	Recommend rephrasing: "To manage cybersecurity risks to critical infrastructure,…"
5	UTC		te	1	88	1	make sure that it is clear that we are after cyber improvements	to achieve "cybersecurity" outcomes

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

6	UTC		te	1	91	1	need to make it clear that this is meant for critical infrastructure even with langauge in intro from EO	add critical infrastructure in front of business
7	UTC		te	1	91	1	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…
8	UTC		te	2	100	1		replace business with enterprise
9	UTC		te	2	102	1	its not just about improving a program	add to measure alignmnet with Framework
10	UTC		te	2	105-106	1	the open process in developing the Preliminary Framework was to develop a robust technical basis to allow organizations to align this guidance with their organizational practices." This statement is a bit confusing as in our view the Framework is consistent with existing standards and best practices and is extremely valuable in	Reword the sentence to point at the Framework process as a process of aligning existing standards and best practices cross-sector which helps demonstrate commonality among those frameworks and assist critical infrastructure owners/operators to align their organizational practices accross different existing frameworks using the NIST framework.
11	UTC		te	2	114	1.1	we are looking to achieve outcomes through the subcategories	change activities to outcomes
12	UTC		ed	2	114	1.1	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
13	UTC		ed	2	116	1.1	Making sentence clearer that there are existing standards	add existing in front of standards
14	UTC		ed	2	123-125	1.1	this sentence appears confusing	Remove sentence This structure ties the high-level strategic view, outcomes…
15	UTC		te	3	143	1.1	This is intended to make it clear that some sectors have standards that are directly applied to them.	add cross-sector and sector specific in front of industry standards
16	UTC		ed	3	145	1.1	Attempting to tie back to the overal posture of cybersecurity.	add posture in front of by comparing

17	UTC		te	3	140-149	1.1	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. Recommend adding clarifying language.
18	UTC		te	3	153	1.1	Making sure to reiterate that this is for critical infrastructure.	add critical infrastructure in front of business/mission
19	UTC		ed	3	155-156	1.1	This is the first reference to a specific section in the introductory material and is somewhat confusing to the reader.	Remove the reference from here or provide references to specific sections where concepts are described for the core, the profile, and the tiers.
20	UTC		te	3	166	1.2	this is a global change to make it clear that this applies to the CI aspects of the organization	Define "organization" as proposed or add critical infrastructure in front of organizations
21	UTC		ed	3	167	1.2	Rewording the sentence.	add needed in front of changes. Replace organizational with their. Add programs after cybersecurity
22	UTC		ed	3	174-176	1.2	These statements were made at the opening of the paragraph.	remove entire opening sentence
23	UTC		ed	3	176-179	1.2	Examples seem to flow well being moved.	move to end of 173
24	UTC		ed	3	177	1.2	ISO 27005 should be ISO/IEC 27005	Replace "ISO" with "ISO/IEC"

25	UTC		te	3	182-183	1.2	We believe that "Because of these differences, the Framework is risk-based to provide flexible implementation" does not communicate the intent of the paragraph. Is the sentence trying to	Consider revising the sentence to clarify.
26	UTC		te	3	181	1.2	Adding cyber to make sure we stay connected to cybersecurity as the outcome.	add cyber in front of security
27	UTC		ed	5	203-205	2	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.
28	UTC		ed	5	207	2	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 pratices" Change activities to outcomes
29	UTC		ed	5	209	2	Adding clarifying word.	add "succesfully" in front of manage
30	UTC		ed	5	216	2	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…"
31	UTC		te	6	218	2	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"
32	UTC		ed	6	227	2	The result is that these are outcomes.	remove high-level
33	UTC		te	6	230	2	A comment below requests 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	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"
34	UTC		ed	6	232	2	This seems like a broad introduction of the Information References.	Change "specific sections" to "existing"

35	UTC		ed	6	235-237	2	Rewording the sentence for clarity.	Reword the senence 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, guidelnes, and practices that are more specific to their sector.
36	UTC		ed	6	238-241	2	This statement seems out of place after completing the introduction of the components of the framework.	Move to a call out box or footnote.
37	UTC		te	6	249	2	Need to keep making it clear that this is related to critical infrastructure	Insert "infrastructure" in front of "functions"
38	UTC		ed	6	251	2		change "or" to "of"
39	UTC		te	6	253	2		change "delivery" to "resilience"
40	UTC		te	7	262-264	2	The detect function iteself 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 Detect function enables timely discovery of cybersecurity events to limit or contain the impact of a potential cyber incident.
41	UTC		te	7	266	2	This is an outcome of effective risk management.	remove (including effective planning)
42	UTC		ed	7	274	2		change "or" to "of"

43	UTC		te	7-8	281-306	2	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. 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 .

44	UTC		te	7-8	307-320	2.4	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. 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:

45	UTC		te	8	332	2.4	We believe that the Framework should acknowledge existence of organizations that have not achieved Tier 1. We propose to create Tier 0 to communicate that. 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.
46	UTC		te	9-10	332-346	2.4	The Tier 1 text has been modified to include the connection to the Framework Functions. 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. o Integrated Program – There is a limited awareness of cybersecurity risk at the organizational level. The organization implements cybersecurity risk

47	UTC		te	10	347-357	2.4	The Tier 2 text has been modified to include the connection to the Framework Functions. 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. o Information Sharing – Cybersecurity information is
48	UTC		te	10	358-370	2.4	The Tier 3 text has been modified to include the connection to the Framework Functions. 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

49	UTC		te	10	371-385	2.4	The Tier 4 text has been modified to include the connection to the Framework Functions. 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. 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
50	UTC		ed	10	386-389	2.4	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 also be a call out box.
51	UTC		te	9	332	2.4	This is alternative text for the Tier 0 definitons that pulls the alignment with the Framework Functions out of the Risk Management Process definition.	• Tier 0: Not Initiated o Tier 1 has not been achieved.

52	UTC		te	9	332-346	2.4	This is alternative text for the Tier 1 definitons that pulls the alignment with the Framework Functions out of the Risk Management Process 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
53	UTC		te	10	347-357	2.4	This is alternative text for the Tier 2 definitons thatpulls the alignment with the Framework Functions out of the Risk Management Process 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

54	UTC		te	10	358-370	2.4	This is alternative text for the Tier3 definitons that pulls the alignment with the Framework Functions out of the Risk Management Process definition.	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. o Integrated Program – There is a formalized approach
55	UTC		te	10	371-385	2.4	This is alternative text for the Tier 4 definitons that pulls the alignment with the Framework Functions out of the Risk Management Process 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
56	UTC		te		307-320	2.4	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.
57	UTC		te	11	396	3, 3.1	Merge 3.0 and 3.1 into one section. The steps would be useful for someone that is reiewing their exisiting program and for someone starting out	remove 3.1 Basic Oerview of Cybersecurity Practices header

58	UTC		te	11	391-395	3	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.
59	UTC		te	11	397-401	3.1	This section has been reworded into the introduction. There is a new Section 3.1 Coordination of Framework Implementaton which came from Section 2.3	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. 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

60	UTC		te	11	402-408	3.1	The statement that the "Framework provides a consice way for senior executives and others to distill the fundamental concepts of cybersecurity risk so that they can asses how identified risks are managed……" is a critical statement of Framework's value. While useful in Section 3, this statement may be more impactful in the Introduction, if the word "functions" is replaced with the word "framework."	Consider modifying the paragraph and moving it to Section 1.

61	UTC		te	11	412	3.2	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. 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. 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

62	UTC		te	13	457	Appendix A	We very much applaud the fact that Cybersecurity Framework references ISO/IEC 27001 Appendix A controls. However, we are puzzled why the Framework does not reference ISO/IEC 27001 risk management processes contained in the main body of the standard. ISO/IEC 27001 treats processes and controls differently than NIST SP 800-53. NIST SP 800-53 places some of the risk management processes inside the controls (e.g., risk assessment) while ISO/IEC 27001 contains risk management processes in the main body of the document and the controls in Appendix A. By not referencing ISO/IEC 27001 risk management processes the Cybersecurity Framework misses critical references that help integrate cybersecurity risk into business risk. Referencing ISO/IEC 27001 processes throughout the Framework Core would help Cybersecurity Framework's integration into business risk. Additionally, ISO/IEC 27001 has been recently substantially restructured and updated making the current references to it currently in the Framework invalid.	Remap the Framework to ISO/IEC 27001:2013 main body and Appendix A.
63	UTC		te	13	457	Appendix A	This section makes up the Framework Core.	Rename to Section 4: Framework Core
64	UTC		te	13	459	Appendix A		change "activities" to "outcomes"

65	UTC		te	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"
66	UTC		te	14		Appendix A, Business Environment	The Category mentions informing cybersecurity roles but the Subcategories are silent on this.	Add a subcategory the addresses informing cybersecurity roles.
67	UTC		te	14		Appendix A, Business Environment	The order of ID-BE functions seems to be somewhat counterintuitive.	Recommend reordering as follows: 1. ID.BE-3 2. ID.BE-4 3. ID.BE-5 4. ID.BE-2 5. ID.BE-5
68	UTC		ed	15		Appendix A, Governance	ID.GV-2 grammar is awkward	Replace "responsibility" rather than "responsibilities."
69	UTC		te			Appendix A, Identify	Risk Assessment and Risk Management Strategy will not be effective without Risk Mitigation and Improvement	Recommend adding a categories to include risk mitigation and imprpovement. Mapping to ISO/IEC 27001 will help identify subcategories for these categories.
70	UTC		ed		16	Appendix A, Access Control	Grammar is awkward.	Remove "are" between "facilities" and "limited"

71	UTC		te		18	Appendix A, Awareness and Training	PR-AT-4 and PR-AT-5 are silent on roles and responsibilities of personnel involved in information security whose responsibilities are outside of physical or information security. These personnel range from IT to legal, HR, shipping and receiving, control systems engineers, etc. These personnel are specific to sectors and companies.	Add a subcategory that addresses other relevant personnel with examples.
72	UTC		ed		24	Appendix A, Analysis	RS.AN-2 - Incomplete sentence	Complete the sentence.
73	UTC		te	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 informaion are identified and managed consistent with their relative importance to risk management practices.
74	UTC		te				Systems, software, hardware, data flows, etc are all identified, but there is no data classification in this Function.	Add a subcategory: For critical instructure, the data and information is classified and labeled
75	UTC		te	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
76	UTC		te	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

77	UTC		te	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
78	UTC		te	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
79	UTC		te	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 …
80	UTC		te	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
81	UTC		te	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 infrastucture, the mission, objectives….
82	UTC		te	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
83	UTC		te	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

84	UTC		te	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 infrastucture, the mission and business objectives and activities are identified, documented, prioritized and communicated
85	UTC		te	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
86	UTC		te	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
87	UTC		te	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.
88	UTC		te	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(ies) are identified, documented and communicated
89	UTC		te	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 responsbilities are established and communicated
90	UTC		te	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

91	UTC		te	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 cyberseucurity practices
92	UTC		et	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
93	UTC		te	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
94	UTC		te	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
95	UTC		te	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
96	UTC		te	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
97	UTC		te	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 cyberseucurity threat and vulnerability risk responses are identified, documented, prioritized for risk response and integrated into the cybersecurity program

98	UTC		te	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 estabished and includes priorities, constraints, risk tolerances, and assumptions to support cybersecurity risk decisions
99	UTC		te	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
100	UTC		te	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.
101	UTC		te	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
102	UTC		te	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.
103	UTC		te	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 infratructure, the identities and credentials for systems and people is identified, documented and managed.
104	UTC		te	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.

105	UTC		te	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.
106	UTC		te	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 infratructure, the access permissions to systems is identified, documented, and managed
107	UTC		te	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
108	UTC		te	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.
109	UTC		te	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
110	UTC		te	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 responsbilities
111	UTC		te	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

112	UTC		te	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 responsbilities
113	UTC		te	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
114	UTC		te	18		Data Secuity (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.
115	UTC		te	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
116	UTC		te	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
117	UTC		te	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 acquistion, implementation, redeployment and destruction is protected based on the risk management strategy
118	UTC		te	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

119	UTC		te	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 informaiton are identified, documented and managed based on the risk management strategy
120	UTC		te	19		PR.DS-6	Covered in PR.DS-5	Remove this requirement.
121	UTC		te	19		PR.DS-7	Covered in PR.DS-3	Remove this requirement.
122	UTC		te	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
123	UTC		te	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
124	UTC		te	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.
125	UTC		te	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
126	UTC		te	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

127	UTC		te	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
128	UTC		te	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
129	UTC		te	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?
130	UTC		te	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
131	UTC		te	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
132	UTC		te	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 vulnerabilty information occurs with appropriate parties
133	UTC		te	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

134	UTC		te	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
135	UTC		te	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
136	UTC		te	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
137	UTC		te	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
138	UTC		te	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
139	UTC		te	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.
140	UTC		te	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

141	UTC		te	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 infrastruture, the physical and logical ports of assets are managed according to the cybersecurity risk management strategy
142	UTC		te	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
143	UTC		te	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
144	UTC		te	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 anomolous communication is detected in a timely manner to support the Respond Function
145	UTC		te	22		DE.AE-2	This requirement does not appear to be different from ID.AM-3.	Remove this requirement.
146	UTC		te	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
147	UTC		te	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
148	UTC		te	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

149	UTC		te	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 suppport incident handling and the Respond Function are identified, documented and managed according to the cybersecurity risk management strategy
150	UTC		te	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.
151	UTC		te	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
152	UTC		te	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
153	UTC		te	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
154	UTC		te	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
155	UTC		te	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

156	UTC		te	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 provers are identified, documented and managed
157	UTC		te	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?
158	UTC		te	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 accoring to the cybersecurity risk management strategy
159	UTC		te	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 anomolous events
160	UTC		te	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
161	UTC		te	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
162	UTC		te	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

163	UTC		te	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 cyberseucrity event information is communicated as part of identified and documented information sharing practices
164	UTC		te	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 cybersecrity risk management strategy
165	UTC		te	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
166	UTC		te	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
167	UTC		te	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
168	UTC		te	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

169	UTC		te	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
170	UTC		te	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
171	UTC		te	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
172	UTC		te	24		RS.CO-5	Included this language in RS.CO-4	Remove this requirement.
173	UTC		te	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.
174	UTC		te	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 cybersecurit detection systems are investigated according to the risk management strategy
175	UTC		te	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

176	UTC		te	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
177	UTC		te	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
178	UTC		te	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
179	UTC		te	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
180	UTC		te	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
181	UTC		te	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
182	UTC		te	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 Respons Plans or from actual detected cybersecurity incidents

183	UTC		te	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 Respose plans from PR.IP-10 are updated from exercising the Response Plans or from actual detected cybersecurity incidents
184	UTC		te	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
185	UTC		te	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
186	UTC		te	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
187	UTC		te	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 Respons Plans or from actual detected cybersecurity incidents
188	UTC		te	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 Respose plans from PR.IP-10 are updated from exercising the Response Plans or from actual detected cybersecurity incidents

189	UTC		te	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.
190	UTC		te	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
191	UTC		te	25		RC.CO-2	Integrated this requirements into RC.CO-1. Public Relations includes reputation management	Remove this requirement.
192	UTC		te	27	478-484	Appendix A, Table 2	This text and Table 2 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
193	UTC		te	36	497	App C	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"
194	UTC		te	36	498	App C	How these were "identified" is unclear, suggest edits to be consisistent with these areas are a discussion starting point, more work needs to be done.	replace "currently identifed" with "listed and discussed below."
195	UTC		ed	36	498	App C		change "These intitial" to "The following"
196	UTC		te	36	498	App C	A list and description is not really a roadmap, but a starting point for discussion.	change "roadmap" to "discussion starting point"

197	UTC		te	28-35	485-492	App B	We agree that Privacy and Civil Liberties needs to be addressed within the Framework; however, the Appendix as presented is not directly correlated with critical infrastructure across all sectors. Additionally, with the importance of ensuring that Privacy and Civil Liberties is considered in the implementation of the Framework, these elements would be better suited directly embedded within the Framework Core.	Recommend creating a new category within the Identify function called Privacy and Civil Liberties. Recommend taking the FIPPs principles and creating subcategories.
198	UTC		te	36	509-516	App 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."
199	UTC		te	36	518-522	App C	Prescriptive discussion, should be sector-specific and not in the NIST Framework.	delete "As a result, …such as a biometric."
200	UTC		te	38	576-584	App 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
201	UTC		te	38-39	616-617	App C	be focused on critical infrastructure cybersecurity activities.	delete "including the Privacy Methodology in Appendix B."
202	UTC		te	39	617-626	App C	A detailed description of the shortcomings of the FIPPs is not needed here, get to 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,"