NIST Cybersecurity Framework (CSF or Framework) 2.0. Comment Matrix

Comment Number	Date	Department	Comment	Location of Change (Page number, Section, Header, Paragraph, Line #)	Critical, Substantive, or Administrative Comment	Suggested Language, if Appropriate
1	11/2/2023	U.S. Department of Health and Human Services	Consider highlighting the concept of risks and opportunities early in the document.	Page 1, Executive Summary	Substantive	
2	11/2/2023	U.S. Department of Health and Human Services	This describes ERM. Why is it not explicitly stated?	Page 2, Line 123	Substantive	
3	11/2/2023	U.S. Department of Health and Human Services	Artificial intelligence is not typically thought of as a "technology environment." Would recommend removing it from this list of communication environments, which it may rely on. Would also recommend listing wired and wireless communication environments, instead of only mobile (recognizing that it is not a complete list).	Page 3, Line 141-142	Substantive	"It also applies to all types of technology environments, including cloud, wired, wireless, and/or mobile."
4	11/2/2023	U.S. Department of Health and Human Services	Document Structure This document contains the following sections and appendices: • Section 2 explains the basics of the Framework Core: Functions, Categories, Subcategories, Implementation Examples, and Informative References. • Section 3 provides an overview of common uses for the Framework, including through Current and Target Profiles, as well as guidance on using the Framework to understand, assess, prioritize, and communicate cybersecurity efforts and cybersecurity supply chain risk management efforts.	Page 4 Line 159-172	Administrative	Can a transition plan template be developed to help organizations use as a guide for migration to CSF 2.0. That can be added to the document structure.
5	11/2/2023	U.S. Department of Health and Human Services	This section explains the basics of the Framework Core. See Appendix C for the Framework Core's descriptions of the Functions, Categories, and Subcategories," refers to Appendix C. However, Appendix C details the different categories and subcategories, and the description of the functions is included in section 2.1. Recommend revising this sentence for clarity.	Page 5, Line 185-186	Administrative	
6	11/2/2023	U.S. Department of Health and Human Services	See Appendix C for the Framework Core's descriptions of the Functions, Categories, and Subcategories. Appendix C does not show the frameworks Core descriptions. It shows the function, category and category Identifier.	Page 5 Line 185-188	Substantive	
7	11/2/2023	U.S. Department of Health and Human Services	Related to the sentence, "Establish and monitor the organization's cybersecurity risk management strategy, expectations, and policy," we recommend discussing explicit and implicit risks that are identified based on the organization and use-cases.	Page 5, Line 192-193	Substantive	
8	11/2/2023	U.S. Department of Health and Human Services	In the sentence, "Use safeguards to prevent or reduce cybersecurity risk," we recommend to use risk controls instead or in addition for safeguards, as it is a widely used term.	Page 6, Line 208	Substantive	"Use risk controls to prevent or reduce cybersecurity risk," or, "Use risk controls and/or safeguards to prevent or reduce cybersecurity risk."
9	11/2/2023	U.S. Department of Health and Human Services	"To form and maintain a culture that addresses dynamic cybersecurity risk, the Functions should be **addressed** concurrently." It is our understating that organizations that is using the framework to identify and meet their cybersecurity needs and ensure the security of their organization would establish those functions, or implement them, not address them. We recommend revising the sentence to use "establish" or "implement" instead.	Page 6, Line 234-235	Substantive	"To form and maintain a culture that addresses dynamic cybersecurity risk, the Functions should be implemented concurrently."
10	11/2/2023	U.S. Department of Health and Human Services	"Risk appetite" is not defined prior to use. Would recommend defining and describing within the document.	Page 8, 277-278	Substantive	
11	11/2/2023	U.S. Department of Health and Human Services	3.4.1. Improving Communication Across the Organization	Page 14 Line 488	Substantive	Top-down communication is important for ensuring that everyone in the organization is aware of the organization's cybersecurity priorities and strategic direction. Bottom-up communication is important for ensuring that the voices of those on the front lines of cybersecurity are heard.
12	11/2/2023	U.S. Department of Health and Human Services	3.4.2. Improving Communication With External Stakeholders	Page 16 Line 533	Substantive	The CSF can be used to develop incident response plans, and to communicate with stakeholders about the status of an incident.
13	11/2/2023	U.S. Department of Health and Human Services	The primary objective of C-SCRM is to extend appropriate first-party cybersecurity risk management considerations to third parties, supply chains, and products and services an organization acquires, based on supplier criticality and risk assessment. Effective C-SCRM requires stakeholders to actively collaborate, communicate, and take actions to secure favorable C-SCRM outcomes. It also requires an enterprise-wide cultural shift to a state of heightened awareness and preparedness regarding the potential ramifications of cybersecurity risks throughout the supply chain.	Page17 Line 565-576	Substantive	
14	11/2/2023	U.S. Department of Health and Human Services	"The Framework Core addresses cybersecurity supply chain risk management in two ways." The text does not clearly identify the "two ways." One is clear, "Govern," but reading the text, it sounds like there are more than one additional way. Would recommend clarifying this section or removing reference to "two ways," and instead saying that the Framework Core addresses…in multiple ways.	Page 17, Line 577	Substantive	The Framework Core addresses cybersecurity supply chain risk management in multiple ways.
15	11/2/2023	U.S. Department of Health and Human Services	4.2 Integrating the Cybersecurity Framework With Enterprise Risk Management Organizations can employ an enterprise risk management (ERM) approach to balance multiple risk considerations, including cybersecurity. By considering cybersecurity risks, such as financial, legal, operational, and reputational risks, organizations can make better decisions about how to allocate resources and prioritize risk mitigation efforts.	Page 20 Line 682-684	Substantive	By considering cybersecurity risks, such as financial, legal, operational, and reputational risks, organizations can make better decisions about how to allocate resources and prioritize risk mitigation efforts.
16	11/2/2023	U.S. Department of Health and Human Services	Section 3.4 discusses the relationship between the different resources and level within the company and includes discussion about senior executives, business process, and implementation. This section does not include a discussion about the independent verification of the process within the company. It is recommended to add a discussion about verification of such processes, ensuring that the reviewers of the processes have sufficient knowledge about security, but were not part of the development of the process such that they can provide an independent review.	Pages 22-23	Substantive	
17	11/2/2023	U.S. Department of Health and Human Services	We recommend including a discussion of trust boundaries within Section 3.4.2, to help clearly define and describe shared responsibilities.	Page 24	Substantive	
18	11/2/2023	U.S. Department of Health and Human Services	Manufacturing industries, including healthcare, use Bill of Materials (BOM) for hardware components. We recommend using BOM in addition to inventory in section 3.5, Managing Cybersecurity Risk in Supply Chains With the Framework. A similar concept was included in the Identify category under Asset management (p.41 table 6). We recognize that BOM would need to be clearly distinguished from Software Bill of Materials (SBOM) to avoid confusion.	Page 24	Substantive	

19	11/2/2023	U.S. Department of Health and Human Services	"GV.RM-07: Strategic opportunities (i.e., positive risks) are identified and included in organizational cybersecurity risk discussions" "Positive Risk" terminology is taken from project management; however, it can be confusing in the context of security and risk management for security. Recommend rephrasing, clarifying or removing it.	Page 31	Substantive	
20	11/2/2023	U.S. Department of Health and Human Services	We recommend specifically discussing end of life (EOL)/decommissioning in the context of risks, third party and supply chain when referring to life-cycle. Failure to plan for timely decommissioning and replacement of outdated, unsupported, and/or non-securable technologies is a known, significant risk.	Page 33	Substantive	
21	11/2/2023	U.S. Department of Health and Human Services	"ID.RA-04: Potential impacts and likelihoods of threats exploiting vulnerabilities are identified and recorded" recommend revising to "exploiting vulnerabilities, or a combination of vulnerabilities"	Page 34	Substantive	exploiting vulnerabilities, or a combination of vulnerabilities
22	11/2/2023	U.S. Department of Health and Human Services	"ID.RA-09: The authenticity and integrity of hardware and software are assessed prior to acquisition and use (formerly PR.DS-08)" Suggest revising to "authenticity, integrity and impact on existing system of ..."	Page 35	Substantive	"The authenticity, integrity, and impact on existing system(s) of hardware and software are assessed prior to acquisition and use"
23	11/2/2023	U.S. Department of Health and Human Services	PR.AA-02-04 discuss authorization and authentication of users and services; however we note that in the context of healthcare some services and users would require an immediate action, such that authenticating them is not feasible. E.g., in emergency rooms where delay in access to devices could risk serious patient harm. We would recommend explicitly recognizing such circumstances, and potential alternatives or a recognition that a deliberate decision will need to be made	Page 36	Substantive	
24	11/2/2023	U.S. Department of Health and Human Services	DE.CM continuous monitoring is discussed only in the context of assets. Many of the organizations that will implement the framework will be manufacturers, that should provide the same level of security for their products. We recommend adding a sub-category and discussing continuous system testing to detect anomalies and vulnerabilities in their products.	Page 40	Substantive	
25	11/2/2023	U.S. Department of Health and Human Services	Incident response reporting and communication doesn't mention of CIRCIA, or other required reporting. It may be worth considering adding language around compliance with all applicable reporting requirements.	Page 42	Substantive	
26	11/2/2023	U.S. Department of Health and Human Services	In regards to Incident Recovery Plan Execution (RC.RP): Restoration activities are performed to ensure operational availability of systems and services affected by cybersecurity incidents, Consider adding a subcategory to address federal requirements for backup method, alternate processing site, testing method, Recovery Time Objective (RTO), and recovery strategy.	Page number 43, Table 10.	Substantive	Consider adding a subcategory to address federal requirements for backup method, alternate processing site, testing method, Recovery Time Objective (RTO), and recovery strategy.
27	11/6/2023	U.S. Department of Health and Human Services	How is CSF 2.0 different from other cybersecurity frameworks?	N/A	General	
28	11/6/2023	U.S. Department of Health and Human Services	What resources are available to help organizations implement CSF 2.0	N/A	General	
29	11/6/2023	U.S. Department of Health and Human Services	Are there any training, webinars planned to educate organizations?	N/A	General	