Deloitte.

March 17, 2023

National Institute of Standards and Technology
100 Bureau Drive, Stop 2000
Gaithersburg, MD 20899
Submitted electronically to cybersecurityframework@nist.gov

Email Subject: Deloitte & Touche LLP Comments on the Draft CSF 2.0 Concept Paper

Dear NIST CSF Team,

Enclosed are Deloitte's comments on the Draft CSF 2.0 Concept Paper. As one of the largest professional services organizations in the United States, Deloitte provides a vast array of information security and privacy services across 2,800 engagements traversing major commercial industries, and 15 cabinet-level federal agencies. We serve our clients by helping them to understand their level of cyber resilience based on their critical assets, threat landscape, and maturity of cyber capabilities. Our comments within reflect this deep experience that has been garnered from helping a broad range of industries and organizations in managing their cybersecurity risk.

We believe that many of the uses and challenges of CSF 1.0/1.1 are being addressed appropriately through the CSF 2.0 Concept Paper and we agree with the approaches the paper outlines for: retaining the current level of detail; integrating the CSF into larger risk management frameworks; and broadening the scope to include non-critical infrastructure sectors. In addition, Deloitte believes that the creation of use cases, by industry and/or function, could better position organizations to leverage CSF 2.0 in setting strategic goals and integrating CSF 2.0 into their enterprise risk management program.

It is our view that many of the challenges cited by participants during the February 2023 Workshop relate to leveraging CSF for uses beyond its intended purpose. In attempting to "implement" CSF in conjunction with detailed, prescriptive instructions, the core flexibility of the NIST CSF could be lost. While leaders in organizations do look for numerical scores to understand their maturity of cyber and privacy capabilities, they often need some flexibility in how these numbers are attained.

During our support of the development of the NIST CSF and carrying through numerous deployments across federal, state, and commercial, we have viewed the CSF as a flexible tool set to help organizations make strategic decisions on how they implement the cybersecurity concepts in their organizations. The CSF Tiers can be an instrumental tool in helping an organization to establish a baseline understanding of their current state of enterprise security and developing an overall strategy for meeting future state objectives. Through customization, CSF Profiles can be tailored to the specifics of an implementation to ensure better alignment with organizations' cybersecurity strategy, or to define an acceptable basis for suppliers. By design, these pieces do not provide implementation specifics; rather they give an organization the ability to establish goals that align to the standards most applicable to their unique environment and industry.

In summary, we highly recommend that in addition to following its current direction, the CSF 2.0 provide specific use cases demonstrating how CSF acts as a bridge between strategy and implementation rather than serving as a stand-alone implementation standard. As such, we believe that guidance developed by NIST should retain the same level of detail in the resulting NIST CSF 2.0, as contemplated in the Concept Paper section 2.1. Other general principles that we agree with in the Concept paper include: Section 2.2, alignment with other frameworks such as the Privacy Framework, the National Initiative for Cybersecurity Education Workforce Framework for Cybersecurity, and the Secure Software Development Framework; Section 2.6 to align with contemporary technology trends, such as Zero Trust, IoT, 5G, and Post-Quantum Cryptography; Section 3.1, the inclusion of notional implementation examples of actionable, defensible activities to achieve the outcomes of the CSF Subcategories to support the CSF deployment by small businesses and others; and finally, we think that the proposed addition of the Govern Function in Section 4.1 would be enhanced by providing a description of how CSF adoption can help to integrate cyber and privacy into broader Enterprise Risk Management activities, as was described previously in NISTIR 8286.

We look forward to seeing the continued growth of the NIST CSF and applaud NIST's efforts to continue driving its transparent and thoughtful evolution.

Respectfully submitted,

Colin Soutar
Managing Director
Deloitte Government and Public Services
Risk & Financial Advisory, Cyber Risk
Deloitte & Touche LLP
[redacted]

The comments contain general information only and Deloitte is not, by means of this submission, rendering accounting, business, financial, investment, legal, tax, or other professional advice or services. This submission is not a substitute for such professional advice or services, nor should it be used as a basis for any decision or action that may affect your business. Before making any decision or taking any action that may affect your business, you should consult a qualified professional advisor. Deloitte shall not be responsible for any loss sustained by any person who relies on this presentation.

As used in this email, "Deloitte" means Deloitte & Touche LLP, a subsidiary of Deloitte LLP. Please see www.deloitte.com/us/about for a detailed description of our legal structure. Certain services may not be available to attest clients under the rules and regulations of public accounting.

Comment Template for: NIST CSF 2.0 Concept Paper

Please submit responses to ***cybersecurityframework@nist.gov*** *by March 17, 2023*

Organization:	*Deloitte & Touche LLP*
Name of Submitter/POC:	
Email Address of Submitter/POC:	

Comment #	**Section**	**Page #**	**Commenter**	**Comment** (Include rationale for comment)	**Suggested Change**
1	Overall	1	Deloitte & Touche LLP	We believe that many of the uses and challenges of CSF 1.0/1.1 are being addressed appropriately through the CSF 2.0 Concept Paper and we agree with the approaches the paper outlines for: retaining the current level of detail; integrating the CSF into larger risk management frameworks; and broadening the scope to include non-critical infrastructure sectors. In addition, Deloitte believes that the creation of use cases, by industry and/or function, could better position organizations to leverage CSF 2.0 in setting strategic goals and integrating CSF 2.0 into their enterprise risk management program. It is our view that many of the challenges cited by participants during the February 2023 Workshop relate to leveraging CSF for uses beyond its intended purpose. In attempting to “implement” CSF in conjunction with detailed, prescriptive instructions, the core flexibility of the NIST CSF could be lost. While leaders in organizations do look for numerical scores to understand their maturity of cyber and privacy capabilities, they often need some flexibility in how these numbers are attained. During our support of the development of the NIST CSF and carrying through numerous deployments across federal, state, and commercial, we have viewed the CSF as a flexible tool set to help organizations make strategic decisions on how they implement the cybersecurity concepts in their organizations. The CSF Tiers can be an instrumental tool in helping an organization to establish a baseline understanding of their current state of enterprise security and developing an overall strategy for meeting future state objectives. Through customization, CSF Profiles can be tailored to the specifics of an implementation to ensure better alignment with organizations’ cybersecurity strategy, or to define an acceptable basis for suppliers. By design, these pieces do not provide implementation specifics, rather they give an organization the ability to establish goals that align to the standards most applicable to their unique environment and industry. In summary, we highly recommend that in addition to following its current direction, the CSF 2.0 provide specific use cases demonstrating how CSF acts as a bridge between strategy and implementation rather than serving as a stand-alone implementation standard. As such, we believe that guidance developed by NIST should retain the same level of detail in the resulting NIST CSF 2.0, as contemplated in the Concept Paper section 2.1. Other general principles that we agree with in the Concept paper include: Section 2.2, alignment with other frameworks such as the Privacy Framework, the National Initiative for Cybersecurity Education Workforce Framework for Cybersecurity, and the Secure Software Development Framework; Section 2.6 to align with contemporary technology trends, such as Zero Trust, IoT, 5G, and Post-Quantum Cryptography; Section 3.1, the inclusion of notional implementation examples of actionable, defensible activities to achieve the outcomes of the CSF Subcategories to support the CSF deployment by small businesses and others; and finally, we think that the proposed addition of the Govern Function in Section 4.1 would be enhanced by providing a description of how CSF adoption can help to integrate cyber and privacy into broader Enterprise Risk Management activities, as was described previously in NISTIR 8286.	N/A
2	2.2 Relate the CSF clearly to other NIST frameworks	5	Deloitte & Touche LLP	NIST should consider integrating Privacy outcomes within the CSF Core and subcategories. Rationale: recent NIST publications (.e.g, 800-53, 800-63-3) recognize that privacy and cybersecurity are integrated efforts. With NIST's stated goal of scoping CSF 2.0 be helpful to organizations regardless of sector/type/size, an increased integration of Privacy could support CSF use cases in industries with larger Privacy concerns (e.g., retail, banking, Federal/state government)	Include references to the Privacy Framework as "Informative References" or more explicitly integrate Privacy considerations/outcomes into core subcategories
3	2.5 Use Informative References to provide more guidance to implement the CSF	6	Deloitte & Touche LLP	NIST should consider second-party vetting of standards mapping provided by other organizations. Rationale: The CSF 2.0 cannot (and should not) map to every applicable cybersecurity standard. The data calls in Sections 1.3 and 2.5 may yield additional resources more broadly applicable but not appropriate for codification in the CSF 2.0 itself.	Update Informational References to include additional applicable standards/mappings from CSF 2.0 Concept Paper data calls.
4	3.1 Add implementation examples for CSF Subcategories	8	Deloitte & Touche LLP	NIST should consider adding the implementation examples in-line within the CSF Core. Rationale: notional examples may be lost in the expanded companion guidance.	Add the national examples in the CSF Core.
5	4.1 Add a new Govern Function	10	Deloitte & Touche LLP	NIST should elevate select subcategories from the existing 'Identify' function to the new 'Govern' function Rationale: Governance activities are included in more than ID.BE, ID.GV, and ID.RM	Include 'Policy' (GV.PO) and 'Risk Management' (GV.RM) as Categories in the new 'Govern' function Move the following subcategories to the new Govern function: ID.AM-6; ID.BE-1; ID.BE-2; ID.BE-3; ID.BE-4; ID.GV-1; ID.GV-2; ID.GV-3; ID.GV-4; ID.RM-1; ID.RM-2; ID-RM-3
6	5.1 Expand coverage for supply chain	11	Deloitte & Touche LLP	NIST should consider expanding the C-SCRM outcomes within the current ID.SC Category in the 'Identify' function Rationale: Integrating C-SCRM across Functions may dilute / duplicate the ID.SC Category, while a stand-alone SC function undercuts that C-SCRM is functionally another form of risk management (though with its own considerations, similar to Privacy)	Expand the C-SCRM outcomes within the current ID.SC Category in the 'Identify' function
7	6.4 Provide additional guidance on Framework Implementation Tiers	14	Deloitte & Touche LLP	NIST should consider removing "external participation" Rationale: Removing external participation may increase the applicability of the Tiers, as not all organizations need to integrate with broad communities (other than for information sharing/threat awareness)	Remove 'External Participation' from Implementation Tiers, or make an optional consideration if it is useful for some use cases.