March 16, 2023

Comments on NIST CSF 2.0 Concept Paper

Thank you for your work on this exciting update to the CSF. Organizations cannot "buy" their way out of the security problem – Cyber is hard, its evolving, resources are stretched thin. Organizations must do better to manage cybersecurity performance to ensure greater visibility into risk, whether basic cyber hygiene is in place, and achieving outcomes that align to the business. Governance and Measurement in cybersecurity are quite possibly the most important factors in effectively managing risk. Bolstering these two areas within CSF 2.0 fosters greater visibility and accountability needed to improve process maturity and consistency of security practices to reduce systemic risk.

We are pleased to submit our comments as part of the process. Do not hesitate to contact us if further discussion is warranted, we are happy to continue our participation in such a worthwhile effort.

Please refer to the comment table below for line-specific comments.

Comment Matrix

Section	Concept Paper Wording	Discussions / Comments	Proposed Wording
1.1. Change the CSF's title and text to reflect its intended use by all organizations	CSF 2.0 will employ the broader and commonly used name, "Cybersecurity Framework" instead of the original "Framework for Improving Critical Infrastructure Cybersecurity."	Consider the inclusion of "Performance" to underscore the importance of governance and measurement to drive desired outcomes.	"Cybersecurity Performance Framework"
3.1. Add implementation examples for CSF Subcategories	-	Concur and to the greatest extent possible, examples should tie to recommended measurements as well to illustrate not only a desired outcome, but how an organization can effectively measure implementation performance and process maturity over time.	-
4.1. Add a new Govern Function	-	Concur and recommend calling attention to the criticality of organizations clearly articulating the linkage from regulatory requirement and business objectives down to the operational metrics that support them. Enabling traceability helps	-

Section	Concept Paper Wording	Discussions / Comments	Proposed Wording
		ensure focus and commitment across the organization and provides the requisite visibility to more effectively achieve desired outcomes.	
4.2. Improve discussion of relationship to risk management	-	Similar to the above in that establishing risk appetite early and at the appropriate levels of the organization will set the stage for more efficient spend in cyber as well as allow for the creation of right-sized measurements of operational cyber effectiveness which in turn most accurately informs risk.	-
6. CSF 2.0 will advance understanding of cybersecurity measurement and assessment	-	Concur on the importance of driving performance-based outcomes around cyber efforts. Linking to 800-55 will help all organizations better understand the importance of measurement as well as how to implement measures in a practical and meaningful way. The Cybersecurity Performance Management (CPM) framework is in alignment with NIST's measurement work and has been endorsed by Gartner, featured in their IT Risk Management Hype Cycle. Recommended NIST start to include CPM as it is becoming the industry standard term.	Cybersecurity Performance Management (CPM)
6.1. Clarify how leveraging the CSF can support the measurement and assessment of cybersecurity programs	-	Measurements, when done right, can do many positive things to include: Help support / provide new visibility into Return on Investment of cyber activities Align the organization with policies and promote a culture of risk management with incentive-based team competition.	-

Section	Concept Paper Wording	Discussions / Comments	Proposed Wording
		Provide greater insight into operational effectiveness of cybersecurity thereby improving understanding of risk Improve process maturity and consistency of security practices Drive behavior	
6.2. Provide examples of measurement and assessment using the CSF	These include: What is the best way to communicate organizational cybersecurity posture to non-cybersecurity audiences? Is the organization's cybersecurity maturity improving? Where does the organization need to improve? How does an organization understand its cybersecurity posture across the organization, aggregating across systems?	This goes back to the comments above in 4.1 where the organization should map cybersecurity performance to higher level organizational goals and business risk. Clearly delineating risk and impact of the business as it relates to a lack of consistent patching within a critical business unit is a must as an example. Mapping operational measures of cybersecurity effectiveness to business objectives is a must to have these conversations effectively and in a timely manner. In a similar vein – operational measures (e.g.: % of users with MFA) provide assurance of coverage and performance providing organizations insights to baseline levels of maturity and a far better understanding of their gaps, providing data informed decisions around priorities and roadmaps to ensure security is applied according to risk appetite and consistently performing at the requisite level. For understanding across systems and geographies it goes back to the basics of governance and inventory / data management. Understanding critical business functions and the underlying IT and data is critical in order to properly "tag" with this detail to include business owner, etc.	-

Section	Concept Paper Wording	Discussions / Comments	Proposed Wording
		This exercise supports recovery and response efforts in addition to the enablement of more useful metrics and measurements across business units and other dimensions that can be tailored to accommodate each organization. On Measurement Terminology: Please refer to TDI's comments on NIST 800-55	
6.3. Update the NIST Performance Measurement Guide for Information Security	-	Consider inclusion of an honest paragraph of "why" we need measurement. Cite evidence that supports the fact that organizations cannot "buy" their way out of the security problem – Cyber is hard, its evolving, resources are stretched thin. Orgs must do better at managing cybersecurity to ensure greater visibility into risk whether or not basic cyber hygiene is in place and providing outcomes that align to the business.	-