Comment Template for: NIST CSF 2.0 Concept Paper

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

Organization:	*Easy Dynamics*
Name of Submitte	*Sarah Villarmarzo*
Email Address of	[redacted]

Comment #	Section	Page #	Comment (Include rationale for comment)	Suggested Change
1	2.5	6	There has been discussion around the topic of aligning the informative references to additional standards, and the balance between helping those that need compliance support versus implementation guidance through this section. We would argue that the subcategory is the "what" and the informative references section provides more of the "how", i.e. the section is more useful as implementation support rather than strict compliance. If there are organizations that need to demonstrate compliance, there is more than likely a separate document(s) they need to be evaluated against. Therefore, we encourage NIST to use the informative references section to provide a broad suite of related items from a variety of external sources.	N/A - observation
2	2.4	6	We applaud the Online Informative References Library tool as a great way to maintain realtime references and guidance, as well as to encourage industry-specific mappings. Perhaps it could be expanded to include general guidance, such as linking users to NIST templates or other publications available, for example the Privacy Risk Assessment Methodology or the National Checklist Program, for additional support to users looking for informative reference materials. Please note - we have not yet explored the full extent of the new Cybersecurity and Privacy Reference Tool and it may be that this tool would meet the need.	N/A - observation
3	2.6	7	Organizations may benefit from seeing which risks a category or sub-category aims to address, to increase their understanding of the intent of the category and help them design/select the best value controls. This suggestion may only be practical in some cases, as many categories and sub-categories address multiple or generalized threats (e.g. incident response planning).	Include links to specific threat classes, e.g. drawing from STRIDE or the CVE database (not to the lowest-level of vulnerability details but if they have a classification system), potentially in supplemental materials.
4	4.2	11	By making the CSF as outcome-focused as possible, organizations will have a better sense of why a certain category is important. This may also help organizations evaluate themselves or gauge the risk associated with an immature implementation in that area. It could be done at the category and/or subcategory level.	Phrase categories and/or subcategories in the following way: "perform X… in order to/to result in Y."
5	6.2	13	NIST may consider structuring the subcategories in a manner that is consumable by OSCAL or other machine-readable formats. This may require a partnership with the OSCAL team to work around non-binary inputs, to accommodate the qualitative nature of some of the subcategories.	N/A - observation
6	6.4	14	Tiers are an important tool for evaluation. If CSF 2.0 includes tiers at the subcategory level (or something more like a maturity model for each item), it would help organizations conduct more detailed self-assessments and identify gap areas which they could then map against their risk profiles to help them prioritize cybersecurity resources. This information could then be summarized to inform the overall Tier. This type of model would not have to be in the core per se, but could be part of a supplemental guide on how to approach a self-assessment of your own security posture using the CSF.	N/A - observation