Comments for: NIST CSF 2.0 Core (Draft)

Organization:	*Easy Dynamics*
Name of Submitter/POC:	*Elysia Calderon, Caitlin Newark*
Email Address of Submitter/POC:	[redacted]

Comment #	Section	Page #	Line(s)	Comment (Include rationale for comment)	Suggested Change
0	General	General	*[provide range]*	The new govern function works well to align with new models for zero trust and policies that agencies and organizations seek to address.	Potentially move continuous improvement and technology resilience to the govern function as well.
1	-	-	-	*The document, while descriptive and informative, may not be sufficiently brief and instructive for all users.*	*Recommend developing a short (<2 pages) set of instructions for applying CSF, written in active and simple language (e.g., "First, do THIS, next do THAT") that would be easily understood by users without an IT/cybersecurity background (i.e., small business owners), who have minimal time and resources available. Could supplement or accompany NIST SP 1271, e.g., as a checklist.*
2	-	-	-	*Implementation tiers could be used as a more informative resource if tiers were characterized further.*	*Recommend developing a suggestive baseline of subcategories for tier 2 through tier 4 to further characterize the rigor of the tiers. This could provide additional guidance for creating current/target profiles and assistance for identifying specific cybersecurity goals for users without cybersecurity backgrounds.*
3	2.1	5	194-195	Opportunity for wording improvement. Current text reads "The GOVERN Function is cross-cutting and provides outcomes to inform how an organization will achieve and prioritize the outcomes…"	Suggest varying use of "outcomes" to eliminate repetition, e.g., "The outputs of the cross-cutting GOVERN Function inform how an organization will achieve and prioritize the outcomes…"
4	2.1	6	216-218	Opportunity for wording improvement. Current text reads "DETECT enables timely discovery and analysis of anomalies, indicators of compromise, and other potentially adverse cybersecurity events that may indicate that cybersecurity attacks and incidents are occuring."	Suggest tightening and varying wording, e.g., "DETECT enables timely discovery and analysis of anomalies, compromise indicators, and potentially adverse cybersecurity events that may signal an attack."
5	2.1	6	229-230	Opportunity for wording improvement. Current text reads "IDENTIFY Functions will support timely incident response and recovery actions for cybersecurity incidents in the RESOND and RECOVER Functions."	Suggest "IDENTIFY Functions support timely cybersecurity response and recovery actions in the RESPOND and RECOVER Functions."
6	3.1.1	10	330	Currently reads "… in Section 1)."	Suggest removing ")"
7	Appendix A	23	744	Currently reads "This appendix provides notional templates that organizations can choose to use and adapt…"	Suggest removing "choose to"
8	Govern	31		GV.SC-04: Opportunity for additional wording. Currently reads "Suppliers are known and prioritzed by criticality."	Suggest adding more wording after "criticality" to specify how organizations should approach identification of suppliers, e.g., "Suppliers are known and prioritized by criticality to business operations."