Comments for: NIST CSF 2.0 Core (Draft)

Organization: *Easy Dynamics*	
Name of Subm *Sarah Villarmarzo, Hannah Posey-Scholl*	
Email Address [redacted]	

Comment #	Section	Page #	Comment (Include rationale for comment)	Suggested Change
1	General	General	We applaud the increased emphasis on outcomes and believe this will be a flexible way for organizations to approach their use of the CSF.	N/A
2	General	General	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.
3	General	General	The general updates regarding supply chain security are good; the core or supporting materials may wish to emphasize more of the transparency aspect.	Potentially emphasize transparency measures, such as using Service Level Agreements or requiring SBOMs/component lists from external services.
4	General	General	We applaud the inclusion of implementation examples and believe this will be a very helpful resource for organizations to see the types of approaches they could take while still being able to tailor implementation to their own needs. It will also be great for profiles - profiles will be able to create very industry-specific implementation examples for each applicable subcategory.	Potentially request industry for support in creating the examples, or point to industry-specific profiles as they are created.
5	General	General	We heard in the workshops this winter that organizations sometimes tend to look at the "related resources" as required controls to meet a given subcategory. We view them more as implementation guidance and examples.	Potentially combine the implementation examples with the related resources, e.g. citing 800-53, ISO etc. controls as additional examples rather than a separate mapping column; or frame them as example references.
6	General	General	We see the general trend to shifting left (towards more protection and early detection rather than response) as positive. For most organizations, however, response will be a big one. Other items that may be considered are: the ability to contain events/malware; specification of a ransomware policy; assigning of privileges to response team; conducting of tabletops/practice exercises; testing systems before deploying; further emphasis on partner suppliers.	Potentially consider items such as: - the ability to contain events/malware specification of a ransomware policy; - assigning of privileges to response team; - conducting of tabletops/practice exercises; - testing systems before deploying; - further emphasis on partner suppliers.
7	Govern	6-7	GV.0C - Consider calling out compliance/policies to the top-level item; consider specifying performance metrics under GV.OC-04 (i.e. that the organization would specify their own metrics, not that NIST would specify for them!).	Potentially call out compliance/policies to the top-level item. Potentially specify performance metrics under GV.OC-04.
8	Govern	7	GV.RM - Consider adding risk identification/categorization processes, either to item -02 (beyond just SCRM) or to item -05. Alternatively, this may be able to be implied throughout the generic roles and responsibilities item as well.	Potentially add risk identification/categorization processes to GV.RM-02 or GV.RM-05.
9	Govern	9	GV.PO-02 - Potentially reconsider wording on this one, as suppliers sometimes have different needs and capabilities than are used internally.	Potentially reword GV.PO-02 to expand application to suppliers.
10	Identify	9-10	ID.AM - Consider adding something around management of user devices (i.e. the "Bring Your Own" approach).	Potentially add BYOD management to ID.AM.
11	Identify	11-12	ID.RA - Consider including a step to categorize information systems as per the RMF, unless that is implied.	Potentially add a system categorization component to ID.RA.
12	Identify		ID.SC-02 - We recommend keeping this subcategory, or at least the identification of component services - it's important to call out transparency measures and you can use an SBOM in the example implementations. Additionally, requirements for secure software development practices with regards to suppliers may be relevant. (As opposed to PR.PS-07, which is not specific to suppliers.)	Potentially retain or reword ID.SC-02 to emphasize transparency documentation and/or secure software development practices.
13	Identify	13-14	ID.IM - Consider moving this subcategory to the governance function.	Potentially move ID.IM to Govern function.
14	Protect	15-16	PR.AA - As identity nerds, consolidating all this into one item hurts our hearts, but this does cover the most critical aspects. Perhaps include something around MFA specifically, since it's a super low hanging fruit, and/or include certificate and key management.	Potentially call-out MFA and certificate/key management in PR.AA.

15	Protect	16-17	PR.DS - While access control is covered in PR.AA, it may be worth calling out for access to data. Also, consider adding the classification/categorization of data as sensitive.	Potentially include access control and data classification in PR.DS.
16	Protect	19-20	PR.PS - This item is potentially overbroad. Implementation examples will likely be important here, but things like network segmentation, firewalls, installing event management services, etc. may be important to mention. (Though, the presence of those services may be implied through the Detect items.)	Potentially further break down PR.PS.
17	Detect	21-23	DE - Now that Detect has been consolidated into one category, it may be appropriate to add content on fraud, if the team finds it appropriate to expand CSF beyond purely security issues.	Potentially include anti-fraud measures under DE, such as automated fraud monitoring and flagging of suspicious indicators.
18	Respond	25	RS.IM - Keeping this subcategory is recommended, as it is important to have lessons learned as part of the response.	Potentially keep RS.IM as is.
19	Recover	25-26	RC.RP - The term planning seems potentially out of place in the Recover function, since this item refers to determining more tactical recovery actions rather than doing true planning, which would be more preventative.	Potentially reword RC.RP category description to describe 'determining' restoration activities rather than 'planning' restoration activities.