From: Herron, Mark F
Sent: Thursday, December 14, 2017 4:13 PM
To: cyberframework <cyberframework@nist.gov>
Subject: Some Feedback on CSF version 1.1, draft 2

After reviewing the new CSF version 1.1, draft 2, I have a couple observations I think might help make it more clear and easier to use.

It seems to me that it's a little confusing to see/visualize the Categories section in the way it is currently presented. This could be improved by copying Figure 1 from between lines 290 and 292, and re-using it after line 350 (just before the 2.2 Framework Implementation Tiers) but with it expanded, to show just the titles of the categories themselves.

For instance, the Identify function section would have:

Identify

- Asset Management
- Business Environment
- Governance
- Risk Assessment
- Risk Management Strategy

And each other function section would have its categories listed too (but only its categories – for a simpler visualization without the added crosswalk complexity later in the document). The initial figure one, for instance, for Identify doesn't have enough lines for that many categories (it only has three in the figure). I found that a little confusing. And the outcome category descriptions that are there, in lines 320-350, are hidden in the wall of words. Another graphic might help make that presentation less obscure or daunting.

Also, I noticed the outcome categories for Respond and Recover (lines 344 and 350, respectively) use the same terms. I found this odd and confusing. I suggest not reusing the words "communications" and "improvements" as outcome categories in the Recover function, but instead use the designations assigned to that function in NIST SP 800-184 (see figure 3-1 on page 17 of the SP 800-184 document). For Recover then, instead of Improvements, use Tactical Recovery, and instead of Communications, use Strategic Recovery. That would make the full set of outcome categories for the Recover function: Recovery Planning, Tactical Recovery, and Strategic Recovery.

Hope that helps, thanks!

-Mark Herron

Mark Herron, MA, CISSP
Chief Information Security Officer
Office of Information Technology
Central Michigan University