[redacted] [redacted]
Subject: EXT :FW: Feedback and comments on "NIST Cybersecurity Framework 2.0 Concept Paper: Potential"
Date: Thursday, March 9, 2023 1:56:06 PM

FYI

[redacted] [redacted]
Sent: Thursday, January 19, 2023 7:08 PM
To: cyberframework <cyberframework@nist.gov>
Subject: Feedback and comments on "NIST Cybersecurity Framework 2.0 Concept Paper: Potential"

Change 1.1: Wholeheartedly agree with the name change as the legacy "Framework for Improving Critical Infrastructure Cybersecurity" name has at times made it difficult for me to convince my colleagues of the value in adopting the CSF (they tend to think it is someone primarily focused on critical infrastructure and N/A).

Change 2.2 and 2.5: I have lead many efforts to employ the CSF (I support DoD clients using the RMF) as a complement to the RMF primarily for the fact that the CSF structure and taxonomy enable a "dashboard view" of a given system's cybersecurity posture. The number one challenge in using the CSF in that manner however has been for the fact that the "informative references" that attempt to link CSF subcategories to RMF (NIST SP 800-53) controls are a very "loose" mapping and require much further analysis and interpretation. I can/will explain more if its unclear what I mean here. But basically, the ability for organizations using RMF (which is a lion's share of US fed gov't entities) to adopt the RMF will always be problematic until the informative-reference/mappings remove a significant portion of this "looseness." To get after this problem could NIST sponsor some working groups "of the willing" to go through the 800-53 informative references and provide more nuanced mappings (I really think we'll have to map to CCIs or sub-portions of each control … I've done much of this work (days and days worth of converting RMF control language to something that more specifically addresses the corollary subcategory) and could contribute what I've done but would want a group to vet and collaborate with.

After typing the above, I read the section "Call to Action – Provide Mappings: NIST welcomes submissions of mappings to the CSF.
NIST encourages authors/owners of relevant cybersecurity resources to connect with NIST 1) to develop mappings to the CSF 1.1 if a mapping does not exist to ease the development of mappings to CSF 2.0, and 2) to coordinate releasing mappings to CSF 2.0." ➔ to respond to this with the mapping I discussed in the section above, where would you like me to send me XLS?

Change 6.2: The XLS I refer to above in "Change 2.2 and 2.5" is formatted and curated in a way to be used as an assessment tool. It is designed to be used to assess a system that is under the RMF and essentially translates the 800-53 informative reference controls' language so they can be used to

assess the level of compliance with various CSF subcategories. I can contribute this XLS if you would like … but I would recommend a 15-30 minute phone meeting so I can explain how to use it and answer questions.

V/R,

William (Bill) Belei, CISSP
Associate Director, Cyber Operations & Resilience Department
The Aerospace Corporation
[redacted]
[redacted]