From: Tracy, Richard
Sent: Tuesday, January 2, 2018 12:26 PM
To: cyberframework <cyberframework@nist.gov>
Subject: CSF v1.1 Draft 2 Comments

In general, I think the revisions to create CSF v1.1 Draft 2 are beneficial.

With that I have three comments to offer for your consideration:

1. Tiers (paragraph 2.2) - Despite the revisions in Draft 2 I still find Tiers difficult to comprehend. As a practical matter, I think most organizations will say they want to be Tier 4. The purpose behind Tiers and why someone would select Tier 2 or 3 instead of Tier 4 is still not clear to me.

2. Gap Assessment Process (paragraph 3.2) - The proposed gap assessment process is helpful. However, from my experience I think some of the steps are out of order. Specifically, I think one should first define a Target Profile then conduct and Assessment, determine Current Profile which will reveal gaps, that drive prioritized Action/remediation Plans. The current proposed seven step gap assessment process has Current Profile being created before the Target Profile. This seems counterintuitive to me.

3. CSF support for 800-171: It seems that the CSF could be used to help organizations operationalize 800-171. That said, it would be helpful if NIST would provide a mapping of 800-171 CUI requirements to the CSF core. Perhaps Appendix A could be updated to reflect this mapping.

Thanks for the continued great work on the CSF initiative.

Sincerely,

Rick Tracy
Chief Security Officer
Telos Corporation