[redacted] [redacted]
Subject: EXT :FW: Comments for NIST CSF v2.0
Date: Thursday, March 9, 2023 1:26:32 PM

FYI

[redacted] [redacted]
Sent: Thursday, March 2, 2023 8:42 AM
To: cyberframework <cyberframework@nist.gov>
Subject: Comments for NIST CSF v2.0

Dear NIST,

As a user of and assessor of the NIST CSF, there are some comments about the current version, which I hope could be considered when making the v2.0 revision.

1. There is a lack of the role Security Architecture has in the CSF.
2. Subcategory descriptions need more context. Example PR.AC-6 "Identities are proofed …". Suggestion - include a normative section which describes in more detail the intent of the subcategory.
3. The Informative References don't seem to necessarily align with the objective. Perhaps, the reference was chosen as it is closest to the subcategory. Using the nomenclature from OLIR (Superset, subset, etc.) might help clarify the relationship.
4. Measurement. Are Implementation Tiers intended at the Organization level or at the Subcategory level. My comment is that the Implementation Tiers mention Risk Management, which tends to be broader than any subcategory.
5. Measurement. Need more information about how to assess an organization
6. Relationship between Subcategory (Objective) with the associated Profile. NIST CSF should discuss the relationship between a Profile and Controls and/or Policy.
7. Supply Chain. Need more context, especially on the Category and Subcategory level. Is Supply chain about Third Parties, or assets acquired/purchased/sold, or both? Without Guidance, an organization may look at this too narrowly.
8. Security Services can end up being spread across multiple Functions/Categories/Subcategories. Example: Vulnerability Management, Threat Intelligence
9. Some subcategories seem to build on previous ones. How does one account for that in measurement? For example, many subcategories rely on Asset Management. If one has a poor
10. Measurement. Most measurement scores seem to measure the maturity of the process. However, if the process is not effective, then it provides less value to the organization. How does one account for both maturity and effectiveness?

I know these are short, but would be willing to discuss them in more detail.

Leon M. Olszewski | [redacted]