[redacted] [redacted]
Subject: EXT :FW: Feedback for NIST CSF 2.0
Date: Monday, March 20, 2023 11:23:52 PM

CAUTION: This email originated from **outside** your organization. Exercise caution when opening attachments or clicking links, especially from unknown senders.

[redacted] [redacted]
Sent: Friday, March 17, 2023 11:41 PM
To: cyberframework <cyberframework@nist.gov>
Subject: Feedback for NIST CSF 2.0

In response to the NIST Cybersecurity Framework 2.0 Concept Paper, I would like to submit the following comments:

1. Please incorporate the learnings from the Cyber Defense Matrix as you build out NIST CSF 2.0.

If you consider looking at NIST CSF 1.1 as a one-dimensional view of cybersecurity, as expressed through the five Functions, NIST should look at the Cyber Defense Matrix (https://cyberdefensematrix.com [gcc02.safelinks.protection.outlook.com]), which adds a second dimension expressed through five asset classes: DEVICES, APPLICATIONS, NETWORKS, DATA, and USERS. This second dimension should be the basis for NIST CSF 2.0.

Through the inclusion of this second dimension, the Cyber Defense Matrix provides a more complete framework and reveals many gaps in the NIST CSF 1.1, which is not clear on what is an “asset.” Because the Cyber Defense Matrix aims to be a comprehensive checklist, to ensure that no asset is overlooked, it is more explicit and specific on what those assets are: DEVICES, APPLICATIONS, NETWORKS, DATA, and USERS. The matrix takes that which is implicit and makes it explicit and forces us to apply all five NIST CSF functions to all five asset classes. This internal consistency of the matrix is what drives much of its utility as a tool for systematically understanding our security environment. In addition, the term “asset” is not left ambiguous in the Cyber Defense Matrix. By being more specific and consistent in defining an asset, the Cyber Defense Matrix can ensure that all potential attack surfaces in an organization are considered.

Because the NIST CSF 1.1 is not clear in defining what is an asset, we end up with many gaps. For example, in the function of IDENTIFY, the NIST CSF refers to "systems, people, assets, data, and capabilities." Systems, people, and data roughly correspond to some of the five asset classes in the Cyber Defense Matrix, but what exactly is an "asset" in this context? Later in the NIST CSF, we see asset management as a category of IDENTIFY (ID.AM [gcc02.safelinks.protection.outlook.com]). There are IDENTIFY subcategories for DEVICES (ID.AM-1), APPLICATIONS (ID-AM.2), and NETWORKS (ID.AM-3) ID.AM-5 touches upon DATA, but only in the context of prioritization. And there is nothing at all for USERS, except for identifying their cybersecurity roles (ID.AM-6). Practitioners know that understanding who our USERS are is a critical part of IDENTIFY, yet the NIST CSF does not explicitly include it. A reference to the USERS asset class does eventually appear under the function of PROTECT in the category of Identity Management, Authentication, and Access Control (PR.AC [gcc02.safelinks.protection.outlook.com]), which lumps them together with systems that lock doors.

Gaps continue to appear as we move into PROTECT. The NIST CSF defines PROTECT as "Develop and implement appropriate safeguards to ensure delivery of critical services." The notion of an asset is even more vague here than in IDENTIFY. What specific asset or classes of assets are being referenced? The NIST CSF does include categories like Awareness and Training (PR.AT [gcc02.safelinks.protection.outlook.com]), which correspond to USERS-PROTECT, and Data Security (PR.DS), which corresponds to DATA-PROTECT. But where are the categories that PROTECT our NETWORKS, APPLICATIONS, or DEVICES? There is a catch-all category of Protective Technology (PR.PT [gcc02.safelinks.protection.outlook.com]), which is defined as "ensuring the security of systems and assets." Perhaps this is where the remaining three asset classes are covered; however, the NIST CSF wording is still vague with respect to defining what exactly is an "asset."

These inconsistencies and vagaries in the NIST CSF make it much more likely that we will unwittingly leave holes in the defense of our assets. By being specific in defining what is an asset, and consistent in applying each of the NIST CSF Functions to them, the Cyber Defense Matrix ensures that the full range of people, process, and technology capabilities can be properly mapped to each asset class. Through this mapping, we can then see gaps in our security posture across our whole environment.

The Cyber Defense Matrix addresses many other areas called out as a Call For Action in the Concept Paper. Some of these are captured in various presentations that I have given at various conferences (https://www.slideshare.net/sounilyu [gcc02.safelinks.protection.outlook.com]) and in a book that I released in 2022 (https://www.amazon.com/Cyber-Defense-Matrix-Navigating-Cybersecurity/dp/B09QP2GSGZ [gcc02.safelinks.protection.outlook.com]). I'm happy to provide a free digital copy of the book for your review.

2. Please avoid using circular or self-referential terms for any definitions or functions.

This happens throughout the framework document, but here are a few examples:

- on page 8 we have "The Recover Function supports timely recovery…".
- ID.BE-1, ID.BE-2, ID.RA-1 all include a form of the word "identify" in defining activities under the function of IDENTIFY
- PR.AC-2, PR.AC-5, PR.DS-1, PR.DS-2 all include a form of the word "protect" in defining activities under the function of PROTECT.

3. Please avoid using other NIST CSF Functions to define a different Function.

This makes the terms such as IDENTIFY and DETECT seem synonymous. For example, the definition of DETECT uses the word IDENTIFY: "Develop and implement appropriate activities to *identify* the occurrence of a cybersecurity event." (Page 45)

4. Ensure consistency in the application of the five functions.

The most egregious example is this inconsistency is DE.CM-8: Vulnerability scans are performed. Vulnerability scanning is an IDENTIFY function rather than a DETECT function. Vulnerability scanning is a core part of how one does ID.RA-1 (identify vulnerabilities), so vulnerability scanning can't be under both IDENTIFY and DETECT.

5. Leverage the PROCESS dimension in the Cyber Defense Matrix instead of adding a sixth Function for GOVERN.

Regarding the inclusion of a new GOVERN Function, it is already captured in the Cyber Defense Matrix as a crosscutting activity across all existing Functions. Governance, by definition, is a process. Instead of adding it as another column, I suggest expressing it in a way that is similar to how process is captured in the Cyber Defense Matrix.