[redacted] [redacted]
Subject: EXT :FW: NIST Cybersecurity Framework 2.0 Concept Paper Feedback
Date: Thursday, March 9, 2023 1:30:30 PM

FYI

[redacted] [redacted]
Sent: Monday, February 27, 2023 1:25 PM
To: cyberframework <cyberframework@nist.gov>
Subject: NIST Cybersecurity Framework 2.0 Concept Paper Feedback

Hi Team,

I would like to start by acknowledging the great value that NIST CSF has provided to the cybersecurity community.

Below are my comments and feedback on the concept paper:

- Section 3 page 8: It is great to have guidance on how to implement the framework however, a key a challenge to many organisations is to show RoI and value of the implementation. Would be great to include guidance or example of how to monitor, track and report on progress, increase in maturity as well as RoI (maybe risk reduction vs investment)
- Section 3.1 page 8/Section 3.2 Page 9: What are the ways to allow for wider community contributions for adding implementation examples and assisting tools? Maybe have a Github repository that would avail this to the wider community and the community can contribute to it continuously.
- Section 4.1 page 11: Below are the areas that I believe should be part of the new Govern function:
    - ID.AM-6
    - ID.BE [gcc02.safelinks.protection.outlook.com]
    - ID.GV
    - ID.RM
    - ID.SC-1

- Section 4.1 page 11: In a world that is moving to AI, automation and DevOps how does the Govern function is integrated into a rapid environment without slowing down the business. Guidance on methods and ways of implementing security governance in a rapidly changing environment without slowing business outcomes should be introduced or referenced.
- Section 5.1 Page 12: Supply Chain should extend to include software such as open source software libraries used in an organisation applications and the applications used by the organisation.

- Section 6.4 Page 14: Implementation tiers are to a degree confusing for many especially small to medium organisations. While they are good at capturing a current state of how far risk is integrated in cybersecurity it confuses these organisations in terms of how to move forward and get better. Tiers could be consolidated and added to become one of the subcategories of Govern functions where an organisation can assess and track their maturity on viewing and managing risks.

Best Regards,
Ahmed Ali