[redacted]

Subject: EXT :FW: CSF 2.0
Date: Thursday, March 9, 2023 1:34:27 PM

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

FYI

[redacted]

Sent: Friday, February 24, 2023 4:59 PM
To: cyberframework <cyberframework@nist.gov>
Subject: CSF 2.0

Hello,
I have been a cybersecurity practitioner for many years and have leveraged CSF extensively in communications with executives and also in structuring and assessing cyber programs in large telecoms and defense contractors and federal/defense clients.

The simplicity of CSF and the lifecycle view is primarily one of the major reasons for its acceptance and widespread use. I would strongly recommend not to make it too complicated - there will be demands from various industries and people who want the latest buzz word reflected in the framework. Not possible and it will only make it harder to use and follow. For example, zero trust is an architecture or design principle and not an activity that you can add to the framework. Multiple (existing controls in CSF) are needed to achieve zero trust.

Saw that you were planning to add Govern as another vertical. The current structure of Identify-protect-detect-respond-recover is a lifecycle view of an asset or vulnerability. So Govern does not fit in that same lifecycle view as Govern cuts across all verticals. Best would be to add it as a horizontal pillar that sits at the bottom of these five vertical pillars.

Adding measurements to show progress and maturity will be helpful as today most big consulting companies have come up with their own methods of measurement and if you switch consulting companies the measurements and maturity from one consulting company to another does not align. These are also very subjective and the assessment score depends on the person doing the assessment - not a very good state. The measurement and maturity can be similar to the 800-53A document instead of being part of the CSF directly.

Supply chain security - saw that you were planning to add this separately. Understand this is in the news due to solar winds and other events. I think this can be easily covered in the existing CSF verticals - I have been able to do that with my current and past organizations. Any asset we have to secure always has a supply chain implication - so whether the asset is built internally or sourced from a supplier, the Identify------recover lifecycle applies. So do not see a need to add supply chain separately, but existing controls can be reworded or made more specific to include supply chain

considerations.

I would welcome the opportunity to be engaged in this revision - I have the time and cycle to contribute and review as necessary.

Regards,

Sunil
CTO/CISO
Xylem Ventures
[redacted]