[redacted]
[redacted]
Subject: EXT :FW: Potential improvements in CSF 2.0
Date: Thursday, March 9, 2023 1:40:56 PM

FYI

[redacted]
[redacted]
[redacted]
To: cyberframework <cyberframework@nist.gov>
Subject: Potential improvements in CSF 2.0

Dear colleagues, thank you for the opportunity to share my suggestion for improvement CSF 1.1. This framework is shown its usability in the improvement of cybersecurity posture in various kinds of organisations worldwide.

1. **Risk framing.** NIST SP 800-30 proposed a brilliant idea to **frame risks** by focusing on the most important in the specific organisational context and later make all assessments, mitigation measures and monitoring only for them and prevent the spread the resources and efforts. I think it would be nice if CSF 2.0 would refer to risk framing in the section "Establishing or Improving a Cybersecurity Program" (page 21 in CSF 1.1).
2. **Risk Tiering.** The CSF 1.1 is not clear enough for **managing risks on all three tiers**, as noted in NIST SP 800-30, and seems to focus primarily on Tier 3 (information systems) risks. I guess that due to current significant geopolitical changes (like the COVID-19 pandemic, the Russia war in Ukraine, the potential war in the Taiwan Strait, etc.), the overfocusing on the Tier 3 risks and diminishing the attention to Tier 1 risks may seriously decrease the cybersecurity posture.
3. **Shared responsibility.** Due to the widespread adoption of public and hybrid clouds, the idea of **shared responsibility** between cloud customer and cloud provider has become common (see, for example, https://aws.amazon.com/compliance/shared-responsibility-model/ [gcc02.safelinks.protection.outlook.com]). and https://learn.microsoft.com/en-us/azure/security/fundamentals/shared-responsibility [gcc02.safelinks.protection.outlook.com]). It would be nice if CSF 2.0 referred to it and explicitly noted the need to implement security controls in the appropriate part of the big picture, keeping the customer fully responsible for meeting the chosen target security profile.
4. **Certification.** It seems to be nice if CSF 2.0 proposed a clear way to certify the specific organisation to meet the chosen security profile and to certify particular individuals who have the skills and experience to build and manage cybersecurity management systems according to NIST CSF.

Hope my suggestions will help to make this world a bit better.

Best regards,

Vsevolod (Sam) Shabad
[redacted]