[redacted]
Subject: EXT :FW: NIST Cybersecurity RFI
Date: Thursday, March 9, 2023 1:44:40 PM

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

FYI

[redacted]
Sent: Wednesday, February 15, 2023 11:03 AM
To: cyberframework <cyberframework@nist.gov>
Subject: FW: NIST Cybersecurity RFI

Sharing here

[redacted]
Sent: Wednesday, February 15, 2023 9:57 AM
To: CSF-SCRM-RFI <CSF-SCRM-RFI@nist.gov>
Subject: NIST Cybersecurity RFI

NIST Cybersecurity RFI

I use the NIST CSF across business sectors for a diverse group of organizations. I've had to simplify the steps to discovery, risk assessment, target profile, implementation, and assessment. This seems to work well for non-security professionals. Simplicity is best for adoption and translation. NIST has robust SPs, for example, SP 800-53, that cover supply chain risk management, risk assessment, etc. Understanding the other SPs in relation to CSF is key.

One of the weak spots within the CSF is the maturity tiers. The qualitative risk assessment heatmap is inefficient. The industry is moving from qualitative assessment to quantitative. Accurately pin pointing the high risks within context requires a more accurate method. Hubbard and Seiersen have done great work in this area and any quality assessor is using quantitative methodology. If NIST fails to put out a quantitative risk assessment special publication, they may develop a legacy reputation in this area.

Gabriel Silva
CISO
PDC Technology

Sent with Proton Mail [gcc02.safelinks.protection.outlook.com] secure email.