Hello,

I am writing you to provide some feedback on the draft NIST CSF 2.0 framework that was released on August 8, 2023.

The "Target Profile" concept is helpful in envisioning a desired future-state cybersecurity posture, and contrasting that goal with the current state security program, however little guidance is provided for the prioritization of security controls as part of remediation efforts. Other frameworks, such as the Center for Internet Security's Critical Security Controls (CIS CSC) and the Payment Card Industry Data Security Standard (PCI DSS), have relevant guidance from their publishing bodies on how entities should approach addressing compliance gaps and associated risk(s). This guidance is leveraged by advisory firms and self-assessing organizations to form cybersecurity roadmaps to develop budgets, plan projects, and dedicate resources to achieve impactful results. To this aim, many organizations and cybersecurity professionals would appreciate NIST's esteemed perspective on strategical remediation.

Thank you for your review and consideration.

Halli Goodman
Security Advisor, Risk & Compliance – Security Advisory Team