[redacted]
To: [redacted]
Subject: cyberframework
Date: Feedback on CSF 2.0 Draft
Thursday, June 1, 2023 2:02:46 PM

Response to Discussion Draft of the NIST Cybersecurity Framework 2.0 Core

This document is in response to the April 24, 2023 request for comments on the Discussion Draft of the NIST Cybersecurity Framework 2.0 core. Andrew Micone is a Security Operations manager in the finance sector and a Futurist who previously participated in previous NIST supply-chain forums as part of the supply-chain and logistics body RosettaNet, the original National Cyber Security working groups at UCSD, at the invitation of NIST to respond to the health care industry vertical for the framework at NCU, and as part of the recent industry feedback session for the National Privacy Framework at BSU. His current academic work is part of the futurist think-tank TechCast, a special project of the Policy Institute at George Washington University. He regularly presents on usage and updates to the National CyberSecurity framework as part of his volunteer work on the board of the ISACA Idaho Chapter.

General Comments

Good job; the Governance breakout in CSF 2.0 better aligns with the staged maturity models like CMMI and should assist with adoption, but let's keep the work done in CSF 1.1 on the implied adoption framework that was never fully built out. That should be built upon more to aid adoption, which could be part of how you present it (e.g., the core of an organization's evolution from a managed implementation to a defined implementation would be what's contained in GOV). This is especially important since the only staged maturity model NIST has been involved in was the CMMC, and from 1.0 to 2.0 that evolved from a CMMI-style staged maturity model to solely an assurance model for use by DoD vendors.

The maturation of risk management framework controls will help promote integrated risk management.

--

Andy Micone
[+] Add me to your address book