From: carmel MT
To: cyberframework
Subject: Comments on NIST Cybersecurity Framework 2.0
Date: Thursday, August 10, 2023 6:28:05 AM

Framework 2.0 aspires to promote long-overdue organizational governance accountability.

My sole comment concerns lines 506-507 on page 15: "As executives establish cybersecurity priorities and objectives based on those needs, they develop a risk strategy that considers risk appetite and addresses expectations, accountability, and resources."

This assertion depends on ethics, neither law nor regulation, to adopt and deploy compliant CSF; it is voluntary. Ethical violations do not threaten incarceration or fines when breached.

Certain legal or regulatory incentives must materialize, and be subject to strict enforcement, to mandate cybersecurity risk management practice compliance. Until that arises, there's no "beef" to motivate CSF deployment.

I suggest a regulation or law that limits indemnification usage for CxOs and governance boards of directors within website or product terms of service. A reduction in commercial impunity scope for incidents such as data breach, technological product liability or privacy compromise will elevate the CSF's "beef" among those who are hired to protect personal data.

For an organization demonstrating Tier-4 Adaptive CSF guidance compliance via independent audit using NIST 800-53, should an incident arise, regulatory enforcement exemption with a get-well plan seems fair. For an organization that fails to comply or shirks implementation of reasonable mitigation to save expenses, throw the book at their governance team for an incident to set an example.