[redacted] [redacted]

Dear NIST Cybersecurity Framework Team,

I hope this email finds you well. First, I would like to thank you for considering and incorporating some of the suggestions from my initial submission into the NIST Cybersecurity Framework 2.0 Discussion Draft. I appreciate your commitment to engaging the cybersecurity community in the development of this critical framework.

I have reviewed the discussion draft and would like to provide additional feedback related to my initial suggestions and the new features introduced in the draft. I believe these points will further enhance the effectiveness and adaptability of the framework:

1. The new structure of the CSF 2.0 Core, including the addition of the Govern Function, provides a more comprehensive view of an organization's cybersecurity posture. However, consider clarifying the relationships between Functions, Categories, and Subcategories, and providing examples or case studies to demonstrate how they work together in practice.

2. The Implementation Examples column in Table 2 is a valuable addition to the framework, offering actionable steps for organizations to achieve desired outcomes. To further enhance this section, consider soliciting feedback from the cybersecurity community on the usefulness and applicability of these examples and expanding the list based on their input.

3. While the framework's alignment with existing standards and practices is essential, consider providing guidance on integrating the CSF 2.0 with other cybersecurity frameworks, such as the ISO/IEC 27001, to help organizations streamline their cybersecurity efforts and avoid duplicative work.

4. The framework now addresses various organizational contexts, such as legal, regulatory, and contractual requirements. To improve this area, consider providing more specific guidance on how organizations can identify, manage, and comply with these requirements, particularly for organizations operating in multiple jurisdictions or industries with unique regulatory requirements.

5. The focus on supply chain risk management is commendable. To further enhance this aspect, consider providing guidance on how organizations can collaborate with their suppliers, vendors, and other third parties to promote a shared understanding of cybersecurity risks and expectations and foster a culture of collective defense.

6. In light of the increasing prevalence of remote work and the use of personal devices for work purposes, consider adding a category or subcategory focused on the security of remote work environments and bring-your-own-device (BYOD) policies. This could help organizations address the unique challenges posed by these trends and ensure the security of their data and networks.

7. To support continuous improvement, consider adding guidance on conducting regular reviews and updates of the framework based on changing cybersecurity threats, technologies, and best practices. This will help organizations stay agile and adaptive in the face of evolving risks.

I hope you find these additional suggestions useful in refining the NIST Cybersecurity Framework 2.0. I appreciate the opportunity to contribute to the development of this vital framework and look forward to its continued evolution.

Best regards,
Shanil Chetty