[redacted] [redacted]
Subject: EXT :FW: NIST Cybersecurity Framework 2.0 Concept Paper Feedback & Suggestions
Date: Thursday, March 9, 2023 1:54:34 PM

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

FYI

[redacted] [redacted]
Sent: Tuesday, January 24, 2023 10:55 AM
To: cyberframework <cyberframework@nist.gov>
Subject: NIST Cybersecurity Framework 2.0 Concept Paper Feedback & Suggestions

Dear Team,

Here are some feedback and suggestions on the concept paper that could be considered:

1. The proposed changes reflect the current cybersecurity landscape and the growing need for adaptability and flexibility in cybersecurity standards, risks, and technologies
2. The proposed changes, such as incorporating more comprehensive risk management and incident response protocols, seem appropriate and necessary. Additionally, considering the integration of emerging technologies, such as IoT and AI, into the Framework would be beneficial.
3. The proposed changes appear to support different use cases in various sectors, types, and sizes of organizations, and take into account the varied capabilities, resources, and technologies of these organizations.
4. Additional changes that could be considered include incorporating more specific guidance and best practices for implementing the Framework in different industries and sectors, as well as providing more resources for small and medium-sized businesses.
5. For those using the current version of the Framework, the proposed changes may affect continued adoption, but it will likely be beneficial in the long term as they would bring the framework up-to-date with the current cybersecurity landscape.
6. For those not currently using the Framework, the proposed changes may make it more appealing and relevant to them as it addresses current cybersecurity needs and concerns.
7. Include more emphasis on the importance of regular cybersecurity training and awareness for employees, to ensure that all staff members understand their roles and responsibilities in protecting the organization's assets.
8. Develop a stronger focus on supply chain security, to address the potential vulnerabilities that may exist in the systems and networks of third-party vendors and service providers.
9. Incorporate more guidance on incident response planning and incident management, including procedures for reporting and responding to security breaches and data breaches, as well as providing a clear incident response plan template for organizations to follow.
10. Develop a more robust system for measuring and evaluating an organization's cybersecurity

posture, including the use of key performance indicators (KPIs) and metrics to help organizations identify areas where they are performing well and areas where they need to improve.

11. Develop a comprehensive program for Cybersecurity Governance, which will cover the governance of the Cybersecurity Framework, policies, standards, guidelines, and procedures to be developed and implemented.
12. Create a more user-friendly interface for the CSF website and resources, to make it easier for organizations to access and understand the information they need to implement the Framework effectively.
13. Develop a comprehensive mapping of the Framework to international and sector-specific standards and regulations, to help organizations understand and comply with the various requirements they must meet.
14. Develop a specific CSF 2.0 standard for Small and Medium Enterprises (SMEs) that will be easy to implement and understand with less complexity and less cost.
15. Develop a more robust system for continuous monitoring and assessment, which will include automated tools and techniques to help organizations identify and mitigate cyber threats in real-time.

Overall, the proposed updates seem to be a step in the right direction in ensuring that the Framework is effective in addressing the current cybersecurity landscape and the needs of different types of organizations.

Yours Sincerely
Shanil Chetty
[redacted]