Synopsis of Differences between NIST Cybersecurity Framework 1.1 and 2.0

Introduction: The NIST Cybersecurity Framework (CSF) is a voluntary framework that provides guidance for managing and mitigating cybersecurity risk. The transition from version 1.1 to version 2.0 reflects evolving cybersecurity challenges, emerging technologies, and feedback from the user community.

1. Structure and Organization:

- **Version 1.1:** The framework was structured around five core functions: Identify, Protect, Detect, Respond, and Recover, which focused on establishing a comprehensive approach to cybersecurity.
- **Version 2.0:** While maintaining the five core functions, 2.0 emphasizes a more integrated and holistic approach, focusing on the interconnections between functions and introducing an enhanced focus on risk management.

2. Stakeholder Engagement:

- **Version 1.1:** Primarily aimed at organizations within critical infrastructure sectors, with a limited scope for broader applicability.
- **Version 2.0:** Expands its audience to include a wider range of stakeholders, such as small and medium-sized enterprises (SMEs), non-profits, and international entities, encouraging collaboration and information sharing across sectors.

3. Guidance for Implementation:

Commented [TT1]: This change was needed because it had a more integrated and holistic approach. With the framework being updated, it aimed for a better management of the interconnection between the core functions. With the enhanced focus on risk management, it can ensure that all organizations can identify potential threats.

Commented [TT2]: This change was needed because it addresses the cybersecurity needs for a broader range of stakeholders. This made the framework more inclusive and versatile. It encourages collaboration and information sharing across the different areas of the sectors.

- **Version 1.1:** Provided a foundational approach but lacked detailed implementation guidance tailored to specific sectors or organizational types.
- **Version 2.0:** Introduces sector-specific implementation tiers and customizable pathways, allowing organizations to adapt the framework more effectively to their unique risk profiles and operational environments.

Commented [TT3]: Version 1.1 lacked the detailed implementation guidance, so a change was needed. Version 2.2 provided an introduction to the implementation tiers and customizable pathways. This made the framework more adaptable for different organizations.

4. Addressing Supply Chain Risks:

- **Version 1.1:** Acknowledged the importance of supply chain risk management but provided limited guidance.
- **Version 2.0:** Places a stronger emphasis on supply chain cybersecurity, providing expanded guidance and best practices to address risks associated with third-party vendors and supply chain dependencies.

Commented [TT4]: Version 1.1 left organization with limited resources to manage their risk associated with their supply chain and outside venders, so it was time for a change. With version 2.0 it introduces an easier way for organizations to implement the framework in a way that suits them and satisfy their needs. This provided a stronger guidance and best way to practice for supply chain in cybersecurity.

5. Integration with Other Standards:

- **Version 1.1:** Offered some alignment with existing standards and guidelines, but integration was not the primary focus.
- **Version 2.0:** Actively encourages alignment with other frameworks and standards, facilitating a more comprehensive approach to cybersecurity that aligns with international best practices.

Commented [TT5]: This change help prompted a better integration with other frameworks and standards. Version 1.1 only limited the framework's effectiveness in providing a comprehensive approach. However, with Version 2.0 it created a more cohesive and effective strategy that will help in cybersecurity and organizations.

6. Emphasis on Measurement and Improvement:

- **Version 1.1:** Focused on establishing cybersecurity capabilities without significant emphasis on metrics.

- **Version 2.0:** Introduces a focus on measuring effectiveness and maturity of cybersecurity practices, promoting continuous improvement and the adaptation of the framework over time.

Conclusion: NIST CSF 2.0 represents a significant evolution from version 1.1, broadening its applicability, enhancing stakeholder engagement, and providing more comprehensive guidance on implementation, supply chain risks, and continuous improvement. This update aims to ensure organizations can better address the dynamic nature of cybersecurity threats in a rapidly changing technological landscape.

Commented [TT6]: This change was made to ensure that all organizations measure their effectiveness and maturity. Version 2.0 focus on promoting continuous improvement on ways to help organizations adopt to framework over time to address better ways on dealing with cybersecurity attacks and threats. Unlike version 1.1 that didn't help organizations adjust to the new framework.