[redacted] [redacted]
Subject: EXT :FW: [External] Re: Change to Previous Submission
Date: Thursday, March 9, 2023 1:28:15 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: Wednesday, March 1, 2023 10:38 PM
[redacted] [redacted]
Subject: Re: [External] Re: Change to Previous Submission

Due to its current stage of development, the wording "International" or "Multi-National" in the name of the CSF (as I previously suggested) may be premature.

However, the CSF is truly an integrated *set of frameworks* that implement the five key functions or phases. Therefore the name "Integrated CSF" or "CSF Integrated" may be more appropriate at the current iteration.

Professor Wilson

[redacted]

[redacted]

LIBERTY UNIVERSITY
Training Champions for Christ since 1971

[redacted] [redacted]
Subject: [External] Re: Change to Previous Submission

You don't often get email from greg.witte@nist.gov. Learn why this is important [aka.ms]

[EXTERNAL EMAIL: Do not click any links or open attachments unless you know the sender and trust the content.]

Greetings, Dr. Wilson, and thank you for your updated comments!

Have a good afternoon,
Greg Witte
Support for the NIST IT Laboratory

[redacted]
Subject: Change to Previous Submission

"Multi-National Cybersecurity Framework" may be more appropriate than "International Cybersecurity Framework". Alternatively, "The Global Cybersecurity Framework".

Dr. Wilson
----
cyberframework@nist.gov

1.1. Change the CSF's title and text to reflect its intended use by all organizations

The proposed title "Cybersecurity Framework" is too broad. There are many national cybersecurity frameworks in use. CSF 2.0 should recognize the international nature of the CSF; i.e., the collaboration of nearly 4,000 participants from 100 countries. A more appropriate title would be "The International Cybersecurity Framework" CSF 2.0. The 2.0 version of the framework should transition the thinking from a national construct to one that is international, which more accurately describes the global work effort and potential use for a global approach for risk and threat management.

1.2. Scope the CSF to ensure it benefits organizations regardless of sector, type, or size
Since the framework is currently used by non-U.S. organization, this approach will need to address to some extent, the requirements of non-U.S. in this category.

1.2. Increase international collaboration and engagement.

This recommendation aligns with items 1.1 and 1.2 in this comment.

2.1. Retain CSF's current level of detail
My recommendation is to automate the framework for higher effectivity and efficiency during implementation. The foundational CSF knowledge currently exists.
The cost to automate CSF 2.0 or a later version would dramatically improve usability.

2.2. Relate the CSF clearly to other NIST frameworks
Other NIST frameworks could find better use and facility, when integrated with an automated CSF.

2.3. Leverage Cybersecurity and Privacy Reference Tool for online CSF 2.0 Core
Integrating these tools into the automated CSF would increase utility and complexity.

2.4. Use updatable, online Informative References
Better facilitated through integrated automation.

2.5. Use Informative References to provide more guidance to implement the CSF
Yes, highly recommended. Automation would be highly useful here also.

2.6. Remain technology- and vendor-neutral, but reflect changes in cybersecurity practices
Yes, highly recommended. Should also be equally flexible for public and private organizations.

2. CSF 2.0 (and companion resources) will include updated and expanded guidance on Framework implementation

Automation would minimize this cost and reach a global audience.

3. CSF 2.0 (and companion resources) will include updated and expanded guidance on Framework implementation

Yes, highly recommended. Opportunity exists to build these capabilities into the integrated automated CSF.

3.1. Add implementation examples for CSF Subcategories

Yes, highly recommended.

3.2. Develop a CSF Profile template

Automation decreases complexity and increases adoption.

1. Improve the CSF website to highlight implementation resources

This will be a major challenge.

4. CSF 2.0 will emphasize the importance of cybersecurity governance
4.1. Add a new Govern Function
Include a GRC (Governance, Risk, and Compliance) module into the suggested automated CSF x.0.

Conclusion: Achieving rapid implementation and benefits requires simplicity in deployment. We're witnessing downsizing as the trend in organizations for the post COVID era. With reduced staff and the high demand for cyber talent, automation is a much-needed capability. Cyber attackers have figured this out and have developed very sophisticated automated tools, methods and technologies. The CSF is an excellent risk management framework; however it needs to keep pace with advancements in technologies, having the capability to integrate/incorporate all the other methodologies and categories that have been developed over the years, and proposed in this concept paper. Developing an automated, highly integrated CSF would be challenging, but is absolutely critical, and will advance the practice of cybersecurity risk management significantly on a global scale.

Thank you for your patience,

Dr. Joe Wilson

Joe Wilson, Ph.D., CISSP
Associate Professor / Liberty University
School of Computational Science and Engineering
Program: Master of Science in Cybersecurity Education
[redacted]