[redacted]

Subject: EXT :FW: CTA: MAPPING - NIST CSF 2.0 feedback
Date: Tuesday, March 21, 2023 1:21:02 PM

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

[redacted]

Sent: Tuesday, March 21, 2023 6:30 AM
To: cyberframework <cyberframework@nist.gov>
Subject: CTA: MAPPING - NIST CSF 2.0 feedback

To the Team at NIST, To Whom it May Concern,

We would like to provide feedback for the NIST 2.0 Concept Paper and respond to the "**Call to Action – Provide Mappings:** *NIST welcomes submissions of mappings to the CSF. NIST encourages authors/owners of relevant cybersecurity resources to connect with NIST 1) to develop mappings to the CSF 1.1 if a mapping does not exist to ease the development of mappings to CSF 2.0, and 2) to coordinate releasing mappings to CSF 2.0*"

In the form of introduction, Centraleyes is an automated Cyber Risk and Compliance platform. Our platform has multiple use cases and a wide range of users, and is a working example of how leveraging the CSF can support the measurement and assessment of cybersecurity programs across industries. It is beyond our scope to mention all the use cases here but more information can be found at: **www.centraleyes.com [gcc02.safelinks.protection.outlook.com]** or provided upon request.

We have developed a keen knowledge of NIST CSF and a methodology for its implementation via the 800-53 controls (based on the Informative References and CSET) in the form of a questionnaire, scoring and remediation. On a simple level, users use this questionnaire to evaluate their alignment with NIST CSF and improve their cyber posture. Additionally, we have developed a SmartMapping technique to cross-walk the NIST CSF controls to other industry standards such as ISO 27001, SOC 2, PCI DSS, NYDFS, and many more. (Today we are using the current version of CSF and Rev 5 of 800-53.) We have used our SmartMapping technique to map the CSF to over 25 global frameworks, standards and regulations.

We would love to be part of the CTA and would be happy to share with you **how we have mapped NIST CSF to more than 25 global frameworks, standards and regulations**. We can

also provide value as a working example, showing how NIST CSF is being practically used as a foundation by companies across the US and globally.

In the meantime, we would like to provide the following feedback.

- 3.1 Add implementation examples for CSF Subcategories: We have found that the more specific and detailed the subcategories are, the more understandable they become and the greater the ability to practically implement them. More detailed category titles and examples allow users to better measure their alignment. If you do find that you would like to keep the category titles high-level, we would greatly appreciate any additional implementation guidance or examples.
- 4.1 Addition of the **GOVERN** function: Our platform currently assesses 1st and 3rd party cyber risk and compliance against the original 5 Functions. We have found that for our purposes, these 5 functions have sufficiently covered the entire gamut of cyber risk and the addition of another function would result in many structural changes to our platform.

We hope our feedback has been useful and we look optimistically forward to working together as part of the NIST CSF community in the development of the new version.

Please do contact us if we can provide information or examples of any of the above, particularly the SmartMapping.

Yours Faithfully,

Deborah Erlanger

Deborah Erlanger
Cyber Security Analyst
[redacted]
w www.centraleyes.com
[gcc02.safelinks.protection.outlook.com]
[gcc02.safelinks.protection.outlook.com]
[gcc02.safelinks.protection.outlook.com]
[gcc02.safelinks.protection.outlook.com]
[gcc02.safelinks.protection.outlook.com]