From: [redacted]
To: [redacted]
Subject: EXT :FW: NIST CSF 2 - comments and feedback
Date: Thursday, March 9, 2023 1:01:33 PM
Attachments: image001.png

FYI

From: Jonathan Sproule [redacted]
Sent: Thursday, March 9, 2023 6:06 AM
To: cyberframework <cyberframework@nist.gov>
Subject: NIST CSF 2 - comments and feedback

Hi,

I am aware that comments are past due, however I have a suggestion that could potentially be used later down the line considering the boat has past.

One area I understand you are reviewing is around measurement. I am a member of the FAIR Institute and there is plenty of great content within the FAIR ontology that can be used to provide that information from a risk reduction value. "How do I know my efforts have reduced risk?" question is of course important to understand by how much have we reduced risk with our new controls and investments. You can read the details more on this, where Jack Jones himself discusses vendors for selecting CRQ tool, and talks about risk reduction value - https://www.fairinstitute.org/resources/understanding-cyber-risk-quantification-the-buyers-guide-by-jack-jones [gcc02.safelinks.protection.outlook.com]

I think the above resource might be helpful, and I'm sure some of your own members are FAIR members also.

I also understand that you have some feedback from industry requesting more information and technical guidance on a number of areas. I think that of course could potentially be provided in the information references perhaps. I think industry needs to be aware that this is a framework, allowing more freedom of choice and not providing the prescriptive detail that a model, or Standard does. There are differences, as I'm sure you are aware.

Risk Management also suffers from a lack of agreed upon terms. If we ask a number of information security, and risk professionals what risk, threat and vulnerability means we often end up with different meanings. Other professions like medicine, do not confuse their own terms, as well as science. Would you take a flight on a plane if you became aware that those building it couldn't agree on the definition of weight or mass etc? I think perhaps this could be reviewed in detail more to "calibrate" if you will the reader when implementing the framework.

That is just some of my thoughts; apologies for missing the actual deadline though. If you would like to discuss any of the above anytime please do reach out.

Thank you,

Jonathan Sproule MBCS CISM CCSP CISSP
Security and Compliance
Global Information Security (GIS)

proofpoint. [gcc02.safelinks.protection.outlook.com]