[redacted]

Subject: Re: NIST CSF v2.0 - Feedback
Date: Friday, May 5, 2023 12:36:43 PM
Attachments: image001.png
Outlook-nabm2a0o.png

Hi Asiya,

I have another suggestion.

The 2.0 draft includes a new section for Policies and Procedures (GV.PO). This is a great addition. I like how the category includes a requirements that policies be established, reviewed, and applied to relevant third parties. The one component I'm not seeing is *compliance with those policies*. Where in the framework should organization's evaluate their own adherence to policies and procedures to ensure they are being effectuated?

Hope that makes sense.

Best,

Joshua Gregg CISSP | He/Him/His | Manager - Information Risk | Enterprise Risk Management
Golden 1 Credit Union
[redacted]
W golden1.com

[redacted]
Sent: Thursday, May 4, 2023 11:40 AM
[redacted]
Subject: [External] - RE: NIST CSF v2.0 - Feedback

Good afternoon,

Thank you for your input. NIST has received your comments and look forward to your continued support as we work on the next stage of the CSF 2.0.

Asiya

From: Joshua Gregg [redacted]
Sent: Wednesday, May 3, 2023 4:19 PM
To: cyberframework <cyberframework@nist.gov>
Subject: NIST CSF v2.0 - Feedback

Good afternoon,

I am reviewing the CSF 2.0 draft and would like to make a few suggestions. 1) In some categories and

subcategories, the phrase "required by law, regulation, or policy" is used. I'd like to recommend a better phrasing. Since a "law" is the umbrella term for any rule we must follow, a "statue" is a law passed by a legislature, and a "regulation" is a law created by regulatory agencies, a better phrasing would be, "required by *statue*, regulation, or policy" or, even simpler, "required by law."

Joshua Gregg CISSP | He/Him/His | Manager - Information Risk | Enterprise Risk Management
Golden 1 Credit Union
[redacted]
W golden1.com