From: **Gerald Auger**
Date: Thu, Apr 20, 2017 at 4:20 PM
Subject: CSF 1.1 Feedback
To: cyberframework@nist.gov

Just a couple comments on the CSF I'd like to see incorporated at some point. I will be at he workshop in May as well if you'd like to discuss further.

1. Guidance in identifying priority and/or critical controls would be useful. I know different organizations have different needs, but some controls are fundamental regardless of business or mission (e.g. system inventory, access control, backups). I found it useful in 800-53 with priority codes to inform decision makers on what should be on the shorter term radar. This is especially true if adoption by small businesses lacking dedicated security staff hope to implement effectively.

2. Guidance on how to ascertain control tier needs. I've helped small businesses implement CSF, and I've made an informed information security decision for them on what an appropriate tier would be (for their current size, business, needs), but I feel there is a gap there if the business is trying to adopt without a security professional to assist.

3. Tangental to CSF, a security control assessment tool should be developed. I have been working on one for supporting my needs, but it has been trying. The CSF is great to map to different control sets, but developing an accessible security control assessment tool that maps to CSF is clumsy and cumbersome. For example, the overlap of controls from 800-53 leads to instances where you have to extract pieces of an 800-53 control (hoping you are taking the right pieces) to map to the CSF control. This can lead to gaps or duplication of controls. This can lead to inaccurate risk assessment values down stream when quantifying threats and their likelihood of exploit based on controls. (This is an area I feel a discussion would be better than a bullet point).

4. The ease of the framework to communicate to leadership is great. Templates or a workbook tool that is designed for capturing control states and 'managing your program' that easily exports to a leadership report could assist in adoption and start to produce a consistent look/feel for that type of report in industry.

Thanks for the opportunity to comment.
Love the framework. Looking forward to Workshop.

Gerry Auger