From: **Dandonneau, Louise**
Date: Mon, Apr 10, 2017 at 8:13 AM
Subject: NIST Cybersecurity Framework 1.1 Feedback.
To: "cyberframework@nist.gov" <cyberframework@nist.gov>

Thank you for allowing an opportunity to collaborate on the document. Below is my feedback and comments.

- Section 3.2 is intended to provide guidance to the framework on how to implement, often organizations struggle to get beyond the freeze of Prioritisation and Scoping. While the first 2 steps are indeed important activities, it is sometimes easier to take the framework and outline what is being done today (don't assess, just understand) once that is complete, then prioritization and orientation can happen. I think defining them as steps as in 1-7 is misleading, you can jump around the steps – I would change steps to activities and indicate that these are the activities that you can do to implement the framework, do them in the order that makes sense to the organization and revisit them frequently to make sure they are on track.

- Threat Intelligence should be its own Category under Identify – this is high level, and meant to demonstrate only: All audits, regulatory interactions are requesting information on threat intelligence programs.

    - Threat Intelligence: The organizations decisions and risk tolerances are based on the cyber threat landscape

        - Subcategory: Threat intelligence processes are identified, established, assessed and managed across by organizational stakeholders

        - Subcategory: Identification, prioritization and communication of threats to the organization

        - Subcategory: Incidents to the organization are analyzed against threats

- Section 4.0 – Measuring and Demonstrating Cyber Security – first off I am very happy to see this section in the framework. We struggle as an industry to get this right in several areas.

    - "The Implementation Tiers, Subcategories and Categories are examples of metrics" – Not really, they are examples of areas where metrics can be determined – RS.CO-1: Personnel know their roles ..is an example of where a metric is difficult to capture, however, if you have a testing program, not that I know any that do, you can validate this metric.

        - Core Framework: overall there is no specific definition information on the subcategories. That is, if I do not know what ID.AM-3: Organizational communication and data flows are mapped means (if am new to following out asset management, there is not a specific place to see the definition. Unless the intent is to use the informative references to get further details?

- Detection:
    - DE.AE-6 (new) – Events of interest/Use cases are documented and understood

• There is no reference to knowing the events of interest (or use cases) that an organization will detect on – I have put it in DE.AE, but not positive it fits.

    - there has been a lot of focus on Hunting, however it is not listed as a capability, there is reactive, proactive Detection – e.g. indicators from industry are validated and researched on (indicator hunting).

- Response:
    - Response Planning (RS.RP) –

• RS.RP-2 (new) – Response plans are tested – *note, could also fit in improvements*

    - There are 3 key terms that are listed in response but are not well defined: I have put what I think they are, but not sure what is intended from a framework perspective

• Response Plan – the documented steps or process that an organization follows to respond to an incident

• Recovery Plan – the documented activities that an organization follows once the response plan identifies a specific issue (commonly called playbook)?

• Response Strategy – is this the documented process steps?

    - Documenting incidents so that they can be learned from is not clearly articulated, they are table stakes yes, however it should be specifically outlined in the response activities, we outline what you need to Plan, but not the what you do as part of the activity in terms of general documentation of an incident.

Please feel free to contact me if my responses are not clear or require further context.

Regards,

Louise Dandonneau