From: **Karen Scarfone**
Date: Mon, Apr 10, 2017 at 5:31 PM
Subject: Feedback on NIST CSF 1.1 draft
To: cyberframework@nist.gov

Hello! I have made some comments on the subcategories based on recent work I performed involving mapping security requirements to the version 1.0 subcategories. Please contact me if you have any questions or need additional information. Thanks!

1. ID.AM does not include a subcategory for inventorying data.
2. It is not clear if ID.AM-2 includes inventorying services. The important resource is often not the software as a whole, but a particular service provided by several pieces of software working in combination. For example, ID.BE-4 and ID.BE-5 focus on critical services. If ID.AM-2 does not include service inventory, either its description should either be expanded or a new category covering this should be created.
3. ID.RA does not appear to identify and document existing security controls that may prevent threats from exploiting vulnerabilities. ID.RA-4 and ID.RA-5 mention likelihoods, but it should be clearer that risk assessment must take into account existing mitigations.
4. Some items, such as PR.AC-1, take into account the entire lifecycle of the control. Other items, such as ID.GV-1, involve the control's initial setup only and do not address the rest of the lifecycle. This should be consistent throughout the subcategories.
5. There is not a clear PR.AT subcategory for training other personnel with important security responsibilities, such as software developers who need to know secure coding principles and techniques.
6. PR.DS protects data-at-rest (PR.DS-1) and data-in-transit (PR.DS-2) but not data-in-use.
7. DE.AE and DE.CM address networks much more than hosts. For example, DE.AE-1 talks about a "baseline of network operations and expected data flows for users and systems", but baselines for operations within a host, baselines for user activity, etc. may also be invaluable. Similarly, DE.CM-1 monitors the network, DE.CM-2 monitors the physical environment, and DE.CM-3 monitors personnel activity, but where is the subcategory for monitoring within hosts (physical or virtual)?
8. The DE.CM categories are too specific in regards to the type of malicious activity that is to be detected. There are many other types of malicious activity not listed here.

--
Karen Scarfone, Principal Consultant, Scarfone Cybersecurity