[redacted] [redacted]

Subject: Fwd: FW: Discussion Draft | NIST Cybersecurity Framework 2.0 Core
Date: Thursday, June 8, 2023 10:21:51 AM

Dear Cheri,

Many thanks for your significant work updating NIST CSF. The draft 2.0 is impressive, with many positive and welcome modifications. The consolidation of subcategories into ID.IM is impressive.

I have a few observations that I hope are helpful:

ID.IM-02 refers to security tests and exercises, but it is not clear whether this includes practice drills of response and recovery capabilities to test whether they are ready and work as planned. The language could be clarified or a new subcategory could be added to ID.IM for stress testing organization's response and recovery plans, process, personnel, and supporting technology.

ID.IM-03 refers to improvements, but it is not clear whether this includes fixing a root cause. The language could explicitly include Remediate Root Cause because it is not sufficient to Identify Root Cause, it is also necessary to fix the problem. Implementation guidance could further articulate the need to address technical root causes as well as policy/procedure/risk-management root causes that led to the technical issue.

PR.DS-11 refers to data, but it is not clear whether this includes telemetry used to monitor IT environments and analyze security incidents. The language could be expanded to include backups of such telemetry because this is necessary for retroactive detection and incident response.

PR.DS could have a subcategory for Data Retention because this is required by regulations. Alternatively, the language of PR.DS-09 could be expanded to include data retention as part of the "lifecycle" of data.

Each function could have its own CO subcategory. RS.CO covers incident response outcomes, security recommendations, and potentially notification required by regulations. Examples of reporting/documentation in each of the other functional areas include:

- ID.CO: risk assessment findings
- PR.CO: compliance reports
- DE.CO: metrics of issues and near misses
- RC.CO: after action review and resolution report

Please let me know if I can be of further assistance.

Take care,

Eoghan