From: **Glenn Zimmerman**
Date: Mon, Apr 10, 2017 at 12:16 PM
Subject: Comments and feedback on draft 1.1
To: "cyberframework@nist.gov" <cyberframework@nist.gov>

Please find attached comments as requested on the website. If you have any questions, please address them to me at this email address.

Thank you for the opportunity to review.

GLENN ZIMMERMAN

Senior Security Architect
FirstNet An Independent Authority within NTIA
U.S. Department of Commerce

[Attachment Copied Below]

Comment #1

- Page # 10
- Line # 370-372
- Item:

  Cyber Supply Chain Risk Management – An organization may not understand the full implications of cyber supply chain risks or have the processes in place to identify, assess and mitigate its cyber supply chain risks
- Comment:

  The actual evaluation of cyber supply chain risk extends far beyond any organization's ability to fully mitigate since this would necessitate control of chip foundry production as well as design for a cradle to grave end to end ability to ensure control.

Comment #2

- Page # 10
- Line # 374-377
- Item:

  Risk Management Process – Risk management practices are approved by management but may not be established as organizational-wide policy. Prioritization of cybersecurity activities is directly informed by organizational risk objectives, the threat environment, or business/mission requirements.
- Comment:

  In addition to process, there must be validation of results conducted both by internal and external evaluation. Otherwise, the process is only theoretical in nature.

Comment #3

- Page # 10
- Line # 386-391
- Item:

  Cyber Supply Chain Risk Management – The organization understands the cyber supply chain risks associated with the products and services that either supports the business mission function of the organization or that are utilized in the organization’s products or services. The organization has not formalized its capabilities to manage cyber supply chain risks internally or with its suppliers and partners and performs these activities inconsistently.
- Comment:

  See comment 1 above

Comment #4

- Page # 11
- Line # 422-424
- Item:

  the organization actively adapts to a changing cybersecurity landscape and responds to evolving and sophisticated threats in a timely manner.
- Comment:

  change timely to a timeframe sufficiently responsive to address the threat

Comment #5

- Page # 12
- Line # 436-439
- Item:

  Cybersecurity risk is clearly articulated and understood across all strata of the enterprise. The organization can quickly and efficiently account for changes to business/mission objectives and threat and technology landscapes in how risk is communicated and approached.
- Comment:

  Awareness of risk is highly subjective and typically not consistent across all levels of an organization. This is an intrinsic limitation and pitfall of virtually any enterprise.

Comment #6

- Page # 15
- Line # 550-552
- Item:

  Step 3: Create a Current Profile. The organization develops a Current Profile by indicating which Category and Subcategory outcomes from the Framework Core are currently being achieved. If an outcome is partially achieved, noting this fact will help support subsequent steps.
- Comment:

  Important to understand this snapshots require regular updating in order to be effective.

Comment #7

- Page # 21
- Line # 748-755
- Item:

  In combination with Informative References, the Framework can be used as the basis for comprehensive measurement. The key terms for measuring with Framework are "metrics" and "measures.13" Metrics are used to "facilitate decision making and improve performance and accountability." The Implementation Tiers, Subcategories, and Categories are examples of metrics. Metrics create meaning and awareness of organizational security postures by aggregating and correlating measures. Measures are

"quantifiable, observable, objective data supporting metrics." Measures are most closely aligned with technical controls, such as the Informative References.

- Comment:

  Quantifying or establishing metrics on cyber security is typically fraught with high levels of subjectivity. The true measure is only found when compromises are already detected. Unfortunately, this is often after the fact once the metrics have all indicated superlative performance while the network may well have been compromised for months.

Comment #8

- Page # 22
- Line #
- Item:

  The ability of an organization to determine cause-and-effect relationships between cybersecurity outcomes and business objectives also depends on the ability to adequately isolate those cybersecurity outcomes and business objectives. This is one of the largest challenges affecting measurement of cybersecurity. Special care must be taken to ensure that a given cybersecurity outcome and business objective truly correlate. Generally, correlating cybersecurity measures to higher-level cybersecurity metrics is easier than correlating cybersecurity metrics to business metrics.

- Comment:

  Extremely difficult to achieve causality of events. This item implies if only organizations try hard enough they can do so. The intrinsic interconnectivity and complexity of a typical enterprise environment does not provide for a simple cause and effect correlation.

Comment #9

- Page # 27
- Table 23
- Item:

  ID.AM-6: Cybersecurity roles and responsibilities for the entire workforce and third-party stakeholders (e.g., suppliers, customers, partners) are established

- Comment:

  Add reference: NIST SP 800-14

Comment #10

- Page # 28
- Table 23
- Item:

  ID.GV-1: Organizational information security policy is established

- Comment:

  Add reference: NIST SP 800-27

Comment #11

- Page # 33
- Table 23
- Item:

  PR.AC-6: Identities are proofed and bound to credentials, and asserted in interactions when appropriate
- Comment:

  Access control should also include ABAC - (Attribute Based Access Control)
  ABAC is a logical access control model that is distinguishable because it controls access to objects by evaluating rules against the attributes of entities (subject and object), operations, and the environment relevant to a request

Comment #12

- Page # 33
- Table 23
- Item:

  PR.AC-6: Identities are proofed and bound to credentials, and asserted in interactions when appropriate
- Comment:

  Authentication Measurement can be introduced as a sub-category The Cyber security framework should be able to provide a methodology to compare authenticators and allow a determination to be made on the selection of appropriate authenticators that are commensurate with assessed risk

Comment #13

- Page #40
- Line #
- Item:

  Security Continuous Monitoring (DE.CM): The information system and assets are monitored at discrete intervals to identify cybersecurity events and verify the effectiveness of protective measures.
- Comment:

  Detection of events does not imply nor indicate effectiveness of protective measures. Many systems generate multiple false positive detections while ignoring actual events. This dependence on event detection often leads to false sense of security regarding the effectiveness of the measures in place.