Cherilyn and NIST colleagues:

Thanks for the opportunity to comment on the NIST revised draft.

In my opinion, the NIST Cybersecurity Framework would be strengthened by including more detail on the importance of understanding, assessing, and mitigating human factors related to Cybersecurity--including both malicious and unintentional risks.

As an overview of the criticality for cybersecurity, please see the attached 2022 peer-reviewed journal article, which is also available online at: https://citrap.scholasticahq.com/article/37321-seven-science-based-commandme nts-for-understanding-and-countering-insider-threats

Additional information on human factors related to malicious and unintentional Cybersecurity risk is available from several government offices including DoD's DCSA and ODNI's NITTF. I'm happy to facilitate connections if needed.

The current Draft NIST Cybersecurity Framework 2.0 provides no useful information or guidance in this area, and includes only one broad note on the need to identify and record "Internal and external threats to the organization"; see Page 34:

IDENTIFY(ID)– Help determine the current cybersecurity risk to the organization

  Risk Assessment (ID.RA):The organization understands the cybersecurity risk to the organization, assets, and individuals

    ID.RA-03:Internal and external threats to the organization are identified and recorded

This email and my recommendations are my opinion, not official feedback to NIST on behalf of any government organization. If you prefer to receive this recommendation as official DoD input, please let me know so I can coordinate it through the relevant DoD authorities.

Regards,
Eric

Eric L. Lang, Ph.D.
Director, PERSEREC
Defense Personnel and Security Research Center (PERSEREC)
Office of People Analytics (OPA) Seaside, CA
████████████████████████████