Response to
NIST AI Risk Management Framework: Second Draft
Call for Comments

Submitted by
National Artificial Intelligence Institute (NAII)
Department of Veterans Affairs (VA)
September 29, 2022

- The White House Office of Science and Technology Policy announced the forthcoming AI Bill of Rights at the VA NAII BRAIN Summit on September 8, 2022. It has similar aim as the NIST AI RMF but satisfies a different goal (support policies and practices around AI to protect American civil rights). It is recommended to update Table 1 to present a comparison between the NIST AI RMF, Executive Order 13960, and the WH AI Bill of Rights once it is released.
- In Appendix B "How AI Risks Differ from Traditional Software Risks", NIST may consider expanding on security and privacy controls from NIST standards (e.g. 800-53 rev5) that have a positive impact on addressing AI risks, either partially or in full.
- Suggestions for *Attributes of AI RMF* (p4):
    - Strengthen number 8 to describe alignment with and a unique risk-based perspective of trustworthy AI principles compared to other federal standards and guidelines, especially EO 13960 and the forthcoming White House AI Bill of Rights.
    - Include an attribute to describe an AI RMF success criterion
- Provide more guidance and detail on risk measurement and stratification (high, medium, low) to support a standardized approach to describing trustworthy AI risk.
- Editorial suggestions:
    - Update subsection 3.2.1 with bullets or integrated the text into fewer cohesive paragraphs
    - Update the last sentence of 3.2.2 to "Conversely, the lowest-risk AI systems and contexts may suggest potentially lower prioritizations."
    - Update headers for subsections 3.2.3 and 3.2.4 to accurately reflect intent of narrative
    - Figure 4 does not appear referenced in the text. Also, the figure suggests most principles are dependent on the "Accountable & Transparent" principle, but that isn't described in the text.
    - The text switches between "Accountable & Transparent" and "Transparent & Accountable".
    - Suggest using the form "Fair and bias in managed", i.e., remove the em-dash.
    - Suggest using bullets in section 4.1 for "Measures of accuracy", "Reliability", and "Robustness or generalizability"
    - Suggest a general reordering of AI RMF principles where "Safe" and "Secure and Resilient" are adjacent since they are very similar in nature.
    - Suggest a general reordering of AI RMF principles where "Fair and Bias is Managed" is adjacent to "Privacy-Enhanced"

Please direct any questions to Dr. John Zachary,