afiniti.

September 29, 2022

VIA E-MAIL
Ms. Elham Tabassi
Chief of Staff, Information Technology Laboratory
National Institute of Standards and Technology
100 Bureau Drive
Gaithersburg, MD 20899
E-mail: AIframework@nist.gov

Dear Ms. Tabassi,

Afiniti welcomes the opportunity to provide its comments in response to the second draft of the National Institute of Standards and Technology (NIST) Artificial Intelligence Risk Management Framework (AI RMF).

Background

Afiniti is the world's leading provider of artificial intelligence (AI) that pairs customers with contact center agents based on how well they are likely to interact. Our patented technology uses AI to identify and predict patterns in human interactions, so we can connect customers with the agents uniquely best-suited to helping them. This leads to better outcomes for both customer experience and company brand. Our technology is proven to deliver measurable improvements to customer satisfaction, agent experience, and business revenue for our clients, which no longer rely solely on traditional queue-based contact center operations. We understand that every customer-agent interaction is an opportunity to build trust, which is critical to developing stronger brand loyalty.

Afiniti takes seriously its mission to create responsible technology and implement its own AI governance framework. As Afiniti's Chief Data Officer and Head of Product recently explained, "having a holistic, responsible AI practice in place addresses this issue of trust. As businesses transform, we need observability, accountability and explainability for all AI uses, all of which drive customer trust."[1] These principles are among the core components of Afiniti's responsible AI program.

Overview of the Second Draft of NIST'S AI RMF

AI RMF Core Principles. Observability, accountability, and explainability are also among the key considerations in NIST's AI RMF. Afiniti commends NIST for its work to create the AI RMF. When

---

[1] "Responsible AI – not sentience – is crucial for today's business transformation," *The Times Business Transformation Special Report*, June 30, 2022, available at https://www.afiniti.com/news/detail/responsible-ai-for-business-transformation.

finalized, NIST's AI RMF will outline the key components of a responsible AI framework that companies and organizations of all sizes may implement voluntarily.

Opportunity for Public Comment. Afiniti commends NIST's decision to welcome public comment, permitting interested stakeholders and others to share AI governance best practices to ensure that NIST promulgates a robust and comprehensive AI RMF. Public comment provides the space and ability for companies, organizations, consumers, and other interested stakeholders to share with NIST any concerns or other considerations about implementing a responsible AI program about which NIST may be unaware.

AI RMF's Adaptability. Afiniti commends NIST for recognizing the importance of making the AI RMF a flexible, iterative standard. In our view, the AI RMF's adaptability is a vital feature of the framework imbuing sufficient flexibility to accommodate the dynamic regulatory landscape and the increasingly fast pace of innovation in the field.

NIST Playbook. Afiniti also appreciates that NIST created the draft Playbook that will accompany the AI RMF as a resource for interested stakeholders to understand better how to identify, assess, and prioritize risks associated with technology. The draft Playbook provides a user-friendly and information-rich resource for organizations and companies seeking to implement key elements of the AI RMF.

Afiniti looks forward to the opportunity to review NIST's proposed "Measure" and "Manage" written guidance in the next iteration of the Playbook. An effective, responsible AI program must be data-driven. In the interest of making AI more transparent and explainable, it is important to include well-defined metrics to measure certain critical elements and risks of any AI technology on a continuous basis. It is our view that measurement tools provide meaningful guardrails throughout the product development lifecycle and post-deployment.

To highlight the importance of the resource material in the Playbook in a user-friendly way, Afiniti recommends that NIST consider embedding links from the relevant pages in the Playbook into the corresponding section of the AI RMF. We also offer the recommendations below for NIST's consideration as it finalizes the AI RMF.

Proposals to Expand the Usefulness of NIST's AI RMF

Incorporate Other NIST Frameworks. Afiniti recommends that NIST explicitly connect the AI RMF with other relevant NIST frameworks, including the NIST Privacy Framework and the NIST Cybersecurity Framework.[2] A responsible AI governance program should account for privacy and cybersecurity considerations. That is because an AI governance program without privacy and cybersecurity

---

[2] Available at https://www.nist.gov/privacy-framework and https://www.nist.gov/cyberframework, respectively.

governance does not adequately mitigate the risks associated with predictive learning technology. It is critical that companies and organizations account for the interconnectedness of these considerations.

Given that these considerations are inextricably tied to AI governance, Afiniti recommends that NIST incorporate by reference its privacy and cybersecurity written guidance allowing organizations, companies, and other interested stakeholders to leverage NIST's tools, strategies, and guidance across multiple risk categories where possible. We further propose that NIST map these frameworks together by referencing applicable privacy and cybersecurity NIST controls where appropriate in the AI RMF. This will allow NIST to maximize the usefulness of its guidance in these critical areas.

Data Governance and Privacy Risk Mitigation Guidance. Afiniti recommends that NIST provide detailed guidance about data governance and privacy risk mitigation best practices. Data governance is a core component of an effective, ethical AI program. For this reason, we have developed internal protocols to assess data governance and privacy risks on an ongoing basis. Given their importance, we recommend that NIST include additional guidance on data governance and privacy risk mitigation in the AI RMF.

Third-Party Considerations. NIST should also consider integrating third-party risk considerations throughout the AI RMF. Recognizing that the use of third-party data or systems may impose additional risk areas in a predictive learning tool, Afiniti designed its responsible AI program to include third-party risk considerations. The current AI RMF draft references third-party risk in several areas, but not others. For example, Section 3.2.1 of the AI RMF, outlining the challenges of risk measurement associated with AI, notes that third-party data or systems can complicate risk management. This contrasts with the current draft of Section 4, "AI Risks and Trustworthiness," which does not reference third-party considerations despite their relevance. Given the potential complications associated with third-party data or systems, companies will benefit from a more robust discussion of this topic throughout the framework.

Responsible AI Is a Whole-Company Effort. Afiniti further proposes that NIST emphasize the important role that strong support and messaging from a company's leadership and key stakeholders have in ensuring the sustainability of a responsible AI RMF. Although Section 6.1 of the second draft of the AI RMF discusses the importance of implementing a culture of risk management and acknowledges the critical role of senior management in setting this tone, this issue deserves further discussion given the important role that each employee has in fostering a responsible AI culture.

To that end, NIST's AI RMF should further emphasize the need for engagement at every level of an organization. Based on our own experience, Afiniti understands that a robust and sustainable responsible AI program requires a whole-company approach to understanding and fostering support for the program throughout the organization. We have designed our responsible AI program to ensure that responsible innovation is a priority across teams within the company, and we strive to nurture an "ethics by design"

culture. NIST should emphasize the importance of a whole-company approach throughout the next AI RMF draft.

Need to Establish Tight Controls, Policies, and Procedures. An effective responsible AI program must have multiple, well-defined lines of defense, as is the case in any effective risk-management governance framework. The process of identifying the responsible AI program's distinct lines of defense and the individuals needed to maintain those lines is immensely valuable in operating an effective program. It also establishes accountability by creating checks and balances among key stakeholders and different lines of defense. Finally, Afiniti notes that establishing these lines of defense furthers the goals of promoting responsible AI and fostering customer trust.

Conclusion

Afiniti thanks NIST again for the opportunity to comment on the second draft of NIST's AI RMF and for considering Afiniti's views. We look forward to further communications from NIST on this subject and to reviewing future drafts of the AI RMF as well as the accompanying Playbook.