Booz | Allen | Hamilton

ARTIFICIAL INTELLIGENCE

ENGINEERING YOUR AI FUTURE

# ARTIFICIAL INTELLIGENCE RISK MANAGEMENT FRAMEWORK

*Prepared exclusively for the NIST Artificial Intelligence Risk Management Framework: Initial Draft Request for Comment*

April 2022

CONSULTING | ANALYTICS | DIGITAL SOLUTIONS | ENGINEERING | CYBER

# 1.0 INTRODUCTION

NIST's leadership in developing a standardized risk framework for AI is critical to promote AI trustworthiness and usefulness while minimizing its potential for adverse outcomes. Booz Allen Hamilton (Booz Allen) is pleased to submit our response to NIST's request for comment on its **AI Risk Management Framework: Initial Draft**. The following input is organized consistent with the areas of interest indicated in the **AI Risk Management Framework: Initial Draft**.

# 2.0 DOES THE AI RMF APPROPRIATELY COVER AND ADDRESS AI RISKS, INCLUDING THE RIGHT LEVEL OF SPECIFICITY FOR VARIOUS USE CASES?

Yes. Figure 3 provides a comprehensive set of considerations for trustworthy AI. The definitions/explanations in Sections 5.x provide the appropriate level of detail for the audience identified on Page 3, lines 8-10.

# 3.0 IS THE AI RMF FLEXIBLE ENOUGH TO SERVE AS A CONTINUING RESOURCE CONSIDERING THE EVOLVING TECHNOLOGY AND STANDARDS LANDSCAPE?

Yes. The considerations for trustworthy AI outlined in Figure 3 and discussed in Sections 5.x will remain relevant for the foreseeable future, regardless of technological advancements or changes in technology standards. Additionally, the **map**, **measure**, **manage**, and **govern** functions are flexible enough to be applied to current and future AI initiatives.

# 4.0 DOES THE AI RMF ENABLE DECISIONS ABOUT HOW AN ORGANIZATION CAN INCREASE UNDERSTANDING OF, COMMUNICATION ABOUT, AND EFFORTS TO MANAGE AI RISKS?

Yes. The information outlined in Figure 3 and discussed in Sections 5.x provide criterion for thinking about various characteristics of trustworthy AI. An organization can use these characteristics as a framework for understanding and communicating risks associated with their AI deployments. The categories/sub-categories under the **map**, **measure**, **manage**, and **govern** functions can assist organizations in managing AI risks.

# 5.0 ARE THE FUNCTIONS, CATEGORIES, AND SUBCATEGORIES COMPLETE, APPROPRIATE, AND CLEARLY STATED?

The functions, categories, and subcategories are well described and organized. Additional information that could be helpful includes:

- A subcategory for defining risk thresholds (perhaps as part of the Map function)
- An explanation of the value of the **Map → Classification of AI System → The specific task that the AI system will support is defined (e.g., recommendation, classification, etc.)** for managing risk. It is clear this subcategory is important in helping an organization understand its use of AI, but less clear how this specific understanding would be applied to managing AI risk.

Finally, the use of the term "supply chain" might be a bit confusing to readers, as "supply chain" is a broad topic with different meanings for different types of professionals. The concept of acknowledging risk introduced by upstream data and/or technology products could be just as easily understood (perhaps more easily understood) by rephrasing the sentence on Page 18, lines 8-10 to read "Governance should address ~~supply chains, including~~ trustworthiness of third-party software or hardware systems and data as well internally developed AI systems." Similarly, the reference to supply chain could be removed from Table 4, Category 6.

# 7.0 DOES THE AI RMF ALIGN WITH EXISTING PRACTICES AND BROADER RISK MANAGEMENT PRACTICES?

Yes, the concepts described in the RMF can, and for some organizations, have already been, integrated into existing risk management practices. At Booz Allen, we have augmented our existing risk management processes to include triggers/controls for those projects implementing or relying on AI. Organizations, like Booz Allen, that have existing frameworks for managing risk may find it most efficient/effective to extend their existing frameworks to include controls for managing the risks associated with AI. Additionally, organizations that have quality initiatives may be able to reduce or mitigate risks associated with implementing and maintaining AI by applying software and process quality best-practices to AI projects.

# 8.0 WHAT MIGHT BE MISSING FROM THE AI RMF?

A prerequisite to effective AI risk governance is a comprehensive understanding of the AI solutions being researched, developed, deployed, and maintained within an organization. In many organizations, AI development is decentralized, which adds complexity to the governance process. NIST may consider adding a subcategory within Table 4, Category 1 for frequently inventorying an organization's AI initiatives[1].

# 9.0 WILL THE SOON TO BE PUBLISHED DRAFT COMPANION DOCUMENT CITING AI RISK MANAGEMENT PRACTICES BE USEFUL AS A COMPLEMENTARY RESOURCE? WHAT PRACTICES OR STANDARDS SHOULD BE ADDED?

Yes. NIST may want to consider contextual examples of how an organization could apply the AI RMF to specific problems or domains (e.g., health, aviation, agriculture, education, transportation, etc.). By illustrating the use of the RMF through examples, organizations can improve their understanding of the RMF and help ensure the RMF is appropriately interpreted and adopted.

# 10.0 CONCLUSION

While the use of almost any tool or technology can result in negative outcomes, AI is increasingly being relied on to drive progressively more important decisions. Booz Allen appreciates NIST's commitment to creating an AI RMF and looks forward to providing additional support for developing responsible risk guidelines that help organizations realize the promise of AI.

[1] The Artificial Intelligence/Machine Learning Risk & Security Working Group (ARIS) published a piece entitled *Artificial Intelligence Risk and Governance* (https://rb.gy/5zbwer) that discusses several topics relevant to the NIST AI RMF, including the need for AI inventories.

## About Booz Allen

Booz Allen Hamilton has been at the forefront of strategy and technology for more than 100 years. Today, the firm provides management and technology consulting and engineering services to leading *Fortune* 500 corporations, governments, and not-for-profits across the globe. Booz Allen partners with public and private sector clients to solve their most difficult challenges through a combination of consulting, analytics, mission operations, technology, systems delivery, cybersecurity, engineering, and innovation expertise.

To learn more, visit BoozAllen.com. (NYSE: BAH)