September 14, 2021

Request for Information: Artificial Intelligence Risk Management Framework
86 Fed. Reg 40810 (July 29, 2021)
Docket # 210726-0151

Overview:

The Boston Consulting Group welcomes the opportunity to respond to the NIST RFI on the Artificial Intelligence Risk Management Framework. We believe that competitive advantage exists at the intersection of data science, technology, people, and deep business expertise. To unlock true power, AI must be woven into processes and ways of working and applied where it really matters.

Response:

The greatest challenges in improving how AI actors manage AI-related risks – where "manage" means identify, assess, prioritize, respond to, or communicate those risks;

AI Risks, much like other risk problems faced by more traditional software products, will vary upon where the AI is deployed. We would encourage that NIST emphasize the importance of design and systems thinking when it comes to AI risk management. This type of thinking, in combination with traditional cybersecurity threat modeling, will allow AI Actors to better understand the AI system will be critical to the identification, assessment, and prioritization of AI risks.

One of the biggest issues that NIST could solve with this framework is the ability to communicate risks effectively. We recommend the first step in doing this is by establishing the definitive meaning behind words, phrases, and concepts that are used frequently in this space but often carry some ambiguity with them. Establishing an AI dictionary would be helpful in enabling AI actors to communicate risk.

How organizations currently define and manage characteristics of AI trustworthiness and whether there are important characteristics which should be considered in the Framework besides: accuracy, explainability and interpretability, reliability, privacy, robustness, safety, security (resilience), and mitigation of harmful bias, or harmful outcomes from misuse of the AI;

The appropriateness of the attributes NIST has developed for the AI Risk Management Framework. (See above, "AI RMF Development and Attributes")

BCG acknowledges and agrees on that the attributes NIST developed for the AI Risk Management Framework are appropriate.

Effective ways to structure the Framework to achieve the desired goals, including, but not limited to, integrating AI risk management processes with organizational processes for developing products and services for better outcomes in terms of trustworthiness and management of AI risks. Respondents are asked to identify any current models which would be effective. These could include – but are not limited to – the NIST Cybersecurity Framework or Privacy Framework, which focus on outcomes, functions, categories and subcategories and also offer options for developing profiles reflecting current and desired approaches as well as tiers to describe degree of framework implementation;

NIST has become an industry leader in structuring and distributing widely adopted cybersecurity and privacy frameworks. The NIST Cybersecurity Framework or Privacy Framework will serve as great models for this endeavor.

How the Framework could be developed to advance the recruitment, hiring, development, and retention of a knowledgeable and skilled workforce necessary to perform AI-related functions within organizations.

Our work has demonstrated the benefits of adopting Responsible AI. We would expect a similar outcome for the AI RMF as highlighted below:

A Stronger Bottom Line. Companies that practice Responsible AI—and let their clients and users know they do so—have the potential to increase market share and long-term profitability. Responsible AI can be used to build high-performing systems with more reliable and explainable outcomes. When based on the authentic and ethical strengths of an organization, these outcomes help build greater trust, improve customer loyalty, and ultimately boost revenues. Major companies such as Salesforce, Microsoft, and Google have publicized the robust steps they have taken to implement Responsible AI. And for good reason: people weigh ethics three times more heavily than competence when assessing a company's trustworthiness, according to Edelman research. Lack of trust carries a heavy financial cost. In the US, BCG research shows that companies lost one-third of revenue from affected customers in the year following a data misuse incident.

Brand Differentiation. Increasingly, companies have grown more focused on staying true to their purpose and their foundational principles. And customers are increasingly making choices to do business with companies whose demonstrated values are aligned with their own. Companies that deliver what BCG calls total societal impact (TSI)—the aggregate of their impact on society—boast higher margins and valuations. Organizations must make sure that their AI initiatives are aligned with what they truly value and the positive impact they seek to make through their purpose. The benefit of focusing strictly on compliance pales in comparison with

the value gained from strengthening connections to customers and employees in an increasingly competitive business environment.

Improved Recruiting and Retention. Responsible AI helps attract the elite digital talent that is critical to the success of firms worldwide. In the UK, one in six AI workers has quit his or her job rather than having to play a role in the development of potentially harmful products. That's more than three times the rate of the technology sector as a whole, according to research from Doteveryone. In addition to inspiring the employees who build and deploy AI, implementing AI systems in a responsible manner can also empower workers across the entire organization. For example, Responsible AI can help ensure that AI systems schedule workers in ways that balance employee and company objectives. By building more sustainable schedules, companies will see employee turnover fall, reducing the costs of hiring and training—over $80 billion annually in the US alone.

Conclusion

BCG looks forward to working with NIST and the various stakeholders that respond to this RFI and attend the subsequent workshops that will lead to the development of the AI Risk Management Framework.

Regards,

Jack Molloy

BCG GAMMA Senior Security Engineer
New York, NY