All comments will be made public as-is, with no edits or redactions. Please be careful to not include confidential business or personal information, otherwise sensitive or protected information, or any information you do not wish to be posted.

Comment Template for Responses to NIST Artifical Intelligence Risk Management Framework

Submit comments by August 19, 2

General RFI Topics (Use as many lines as you like)	**Response #**	**Responding organization**	**Responder's name**	**Paper Section (if applicable)**	**Response/Comment (Include rationale)**	**Suggested change**
Responses to Specific Request for information (pages 11,12, 13 and 14 of the RFI)						
1. The greatest challenges in improving how AI actors manage AI-related risks – where "manage" means identify, assess, prioritize, respond to, or communicate those risks;	In order to understand the AI-related risks that impact AI deployment, we need to adequately model the risks. With respect to security, privacy and fairness, we especially need to understand and model the realistic threats. So that different options ranging from how models are built to deployment scenarios could be considered.	University of Texas at Dallas	Murat Kantarcioglu	Please see the attached paper.		
2. 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;	To my knowledge, these are main criteria considered in current practice. Still, I believe robustness to attacks such as poisoning or test time attacks need to be one of the important principles to be considered.	University of Texas at Dallas	Murat Kantarcioglu			

3. How organizations currently define and manage principles of AI trustworthiness and whether there are important principles which should be considered in the Framework besides: transparency, fairness, and accountability;						
4. The extent to which AI risks are incorporated into different organizations' overarching enterprise risk management – including, but not limited to, the management of risks related to cybersecurity, privacy, and safety;	Clearly, there is important synergy between cybersecurity, privacy and AI risks. For example, a cyber attack may be used to poison an AI model training data to insert backdoors into the AI model.	University of Texas at Dallas	Murat Kantarcioglu			
5. Standards, frameworks, models, methodologies, tools, guidelines and best practices, and principles to identify, assess, prioritize, mitigate, or communicate AI risk and whether any currently meet the minimum attributes described above;	I believe we need a new risk management framework that is tailored to different aspects of AI deployment ranging from the data collection to model building.	University of Texas at Dallas	Murat Kantarcioglu			
6. How current regulatory or regulatory reporting requirements (e.g., local, state, national, international) relate to the use of AI standards, frameworks, models, methodologies, tools, guidelines and best practices, and principles;						
7. AI risk management standards, frameworks, models, methodologies, tools, guidelines and best practices, principles, and practices which NIST should consider to ensure that the AI RMF aligns with and supports other efforts;	Please the attached summary of such a proposal.	University of Texas at Dallas	Murat Kantarcioglu			
8. How organizations take into account benefits and issues related to inclusiveness in AI design, development, use and evaluation – and how AI design and development may be carried out in a way that reduces or manages the risk of potential negative impact on individuals, groups, and society.	I believe that every aspect of the AI pipeline need to be revisited for understanding these risks.	University of Texas at Dallas	Murat Kantarcioglu			

9. The appropriateness of the attributes NIST has developed for the AI Risk Management Framework. (See above, "AI RMF Development and Attributes");	I think it is a great start. It may need to be tweaked as different needs are discovered.	University of Texas at Dallas	Murat Kantarcioglu			
10. 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; and						
11. 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.						
12. The extent to which the Framework should include governance issues, including but not limited to make up of design and development teams, monitoring and evaluation, and grievance and redress.						