**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, 2021:**

| **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; | | University of Florida | Erik Deumens deumens@ufl.edu | | 1. The greatest challenge in managing AI related risk is the inherent confusion of the performance of AI, algorithms running on machines, with the performance of humans on comparably complex tasks. This causes the judgement of actors to be biased, leading, in turn, to incorrect assessments on risk. 2. The second major challenge is acknowledging and managing the limitations on AI applications. AI models are heavily reliant on training data and the data collectors. The quality of the models is closely associated with the robustness and the fairness of the data. | Guidance and training nees to be provided to help objectify performance of AI and its limitations so that actors can assess risk more accurately. For AI systems, the data assumptions and model application limitations should be carefully defined to avoid unintended consequences and the societal harms that the AI system may cause. |
| | | | | | | |

| | | | | | | |
|---|---|---|---|---|---|---|
| 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; | | University of Florida | Erik Deumens<br>deumens@ufl.edu | | The characteristics of AI trustworthiness should include "culture-aware" and "inclusiveless". AI system's reliance on the data source makes it very likely to be biased. If the data comes from certain demographic, the analysis can be skewed and result in harmful outcome for different demographic/social/cultural groups. | The characteristics of AI trustworthiness should include culture-awareness and inclusivity. |
| | | | | | | |
| 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; | | University of Florida | Erik Deumens<br>deumens@ufl.edu | | Because AI is asked to perform very complex tasks, it is often hard to define whether an AI performs consistently and relaibly on all tasks within the scope of the design/training of the AI. | In addition to transparancy, fairness, and accountability, the principle of consistency or reproducibility or reliability should be added to assess AI trustworthiness. |
| | | | | | | |
| 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; | | University of Florida | Erik Deumens<br>deumens@ufl.edu | | At the University of Florida, risk assessment of AI software and projects includes assessment of the data to be used for training. | |
| | | | | | | |
| 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; | | | | | No comment | |
| | | | | | | |

| | | | | | | |
|---|---|---|---|---|---|---|
| 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; | | University of Florida | Erik Deumens deumens@ufl.edu | | One major challenge is the lack of standards, policies, or regulations on AI reference data sharing and use. Many institutions and individual publish AI reference/training data in various forms (pictures, texts, and videos, etc.) on websites, a lot of them have people identifiable picutures, voices, locations. Some websites have loosely defined user agreements for data downloading and some don't have any restrictions at all, which pose risk on privacy violations and data misuse. | To mitigate reference data misuse and enable safe and secure data sharing , it is critical to define policies and guidelines on publishing, downloading, and use of data. |
| | | | | | | |
| 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; | | | | | No comment | |
| | | | | | | |
| 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. | | University of Florida | Erik Deumens deumens@ufl.edu | | Ethical and fair AI is an critical component in AI system development and application. To tackle the ethical problems that embedded in AI system design, development, and usage, AI ethics must be systematically applied in the entire AI ecosystem. | AI ethics must be systematically applied in the entire AI ecosystem. 1) Staff hiring - the need to hire a diversified  team. 2) Staff training - develop AI ethics training program and build inclusive workforce with high level AI ethics principles. 3) System and data validation - Create ethical standards and measurements for data collection and the performance of AI systems. |
| | | | | | | |
| 9. The appropriateness of the attributes NIST has developed for the AI Risk Management Framework. (See above, "AI RMF Development and Attributes"); | | University of Florida | Erik Deumens deumens@ufl.edu | | The proposed attributes appear appropriate. | |
| | | | | | | |

| | | | | | | |
|---|---|---|---|---|---|---|
| 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 | | | | | No comment | |
| | | | | | | |
| 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. | | | | | The framework needs to provide guidance on training and education packages to be developed and tailored to different levels in the organization, from senior mangement level to staff who perform different AI functions. | Inclusivity and focus on diversity needs to be present at all stages of development and operation of the framework for risk management around AI. |
| | | | | | | |

| | | | | | | |
|---|---|---|---|---|---|---|
| 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. | | University of Florida | Erik Deumens<br>deumens@ufl.edu | | The connection between the design of AI systems and algorithms and the performance of these systems is much more complex than in any other field of software and systems engineering. As a result, the developer does not and cannot be expected to be cognizant of the implications of their design decisions. Some governance process needs to be developed to ensure that design decisions do not introduce fatal flaws into the systems. These fatal flaws, when detected late in the quality assurance stage or in the field after the products are released in the market are a major part of risk management for AI systems. | The risk management framework should include guidelines for how the loop between engineering AI systems and alogorithms and the performance characteristics of these AI systems in real-life situations can be closed. One can think of a sort of agile devleopment cycle that not only includes the developers and the customers, but also a team performing the task of auditing the performance of AI against the characterisctics and principles of AI trustworthiness listed above. |