Response to NIST RFI on Artificial Intelligence Risk Management Framework

First of all, we thank you for all your time in checking this proposal and would like to introduce what we are doing for securing trustworthy Artificial Intelligence (AI).

TTA(Telecommunications Technology Association) continues to compile technical requirements for implementing trustworthy artificial intelligence. In February, it published a "Development Guide for Trustworthy Artificial Intelligence". It was a research project led by the Korean government.

The above guide contains technical principles/requirements and various examples for stakeholders who want to develop or operate artificial intelligence. This technical principle was derived based on technical documents from the international community and governments that have been published over the past two years, including the EC, UNESCO, and IEEE. Subsequently, the feasibility and applicability were secured through numerous reviews by industry and academic experts in Korea.

This year, we would like to conduct case studies based on this draft. The goal is to create a more industry-friendly and research-friendly guide through a bottom-up approach to fine-grained work that cannot be solved by the traditional top-down approach. At the same time, it will take a lot of effort to match the compatibility with international discussions.

I'm so happy that our efforts and NIST are also in the same context.
Even after NIST's RMF is published early next year, continuous improvement and collection of opinions are expected. I think TTA's efforts and case studies will also be of great help in this process.

This comment paper is about the 2nd draft released by NIST. Please have a look at it and if you have questions feel free to contact us.

Your sincerely,

Junho Kwak, TTA

Comment#1: Taxonomy of risk management

In this document, MAP, MEASURE, and MANAGE are presented as the cores of risk management. This seems to correspond to the risk identification, analysis, evaluation, and treatment specified in the risk management process of ISO 31000. However, it is considered to be less compatible by using terms different from international standards.

Comment#2: Related standards of characteristics of Trustworthiness

Safety, security, and reliability are already well-defined concepts in existing systems engineering academic frameworks. For example, for safety, IEC 61508 defines a safety process for functional safety and is widely used in the industry.

However, there is no mention of this in this document, and for standards defined previously, there is no guidance on how to link them to the risk management systems defined in this document.

In the case of developers and evaluators working in existing industries, the usability of this document will be questioned if there is no guidance.

Comment#3: Contents of Subcategory

Category and subcategory are well listed in this document. However, the content described in the subcategory is still highly abstract. In the actual work, it will be necessary to be more specific about what output to prepare and what action items to prepare.

Comment#4: Use case profiles

In the case of Use case profile, there will be two main purposes. The first goal is a more specific guide to RMF content. The second objective is the detailed supplementation and improvement of the items specified in the RMF. TTA is also conducting an analysis for these two goals while conducting a case study.

In particular, it accepts a lot of technical and realistic feedback from industry experts. For explainability, practical challenges exist because XAI technology is not fully applicable for all AI algorithms. Therefore, AI developers are presenting a number of opinions on the level of applying explainability and various alternative measures of explainability.

I hope that NIST's RMF also have a mechanism to continuously review practical applicability, technical validity, and effectiveness through collection and analysis of use case profiles.