September 28, 2022

TO:
National Institute of Standards and Technology
100 Bureau Drive
Gaithersburg, MD 20899
Submitted electronically to AIframework@nist.gov

From:
Roy Sugimura (PhD)
The Head of ISO/IEC JTC1/SC42 Mirror Committee
Japan

To Whom It May Concern:

Response to NIST Request for Public Comment regarding NIST AI Risk Management Framework Second Draft

Thank you for this opportunity to comment on the NIST AI Risk Management Framework Second Draft.

We believe NIST is generally on the right track as it develops the AI RMF. This second draft of the AI RMF is highly complete. However, there are still many operational hurdles to the AI RMF, such as the need for knowledge background for operations, mixed understanding and interpretation, and significant differences in awareness of its use in different industries, with some optimistic and others less so.

Therefore, we would like to propose the following points that would make the AI RMF easier to use in organizations and further enhance.

Public Comment #1:
Harmonization of AI RMF
Comment:
"The goal of the AI RMF is to offer a resource for improving the ability of organizations to manage AI risks to maximize benefits and to minimize AI-related harms to individuals, groups, organizations, and society. "it states, however, Risk management for AI is being developed in US, Japan, and EU, but is not harmonized yet. Is that good enough as a borderless ECO system for society?

Operating AI risk management with different content in parallel places a tremendous burden on the organization. We believe it is necessary to harmonize them wherever if it is possible in some form in the future.

We also need to ensure that there are no barriers to international standardization, impediments to the development and deployment of AI systems, and gaps in opportunity.

In the second draft, it is not clear how it relates to international standards; to avoid potential confusing AI RMF users, for example, we propose to add the relation of the AI RMF and international standards in the main body of the AI RMF, as shown in ”Table 1: Mapping of AI RMF taxonomy to AI policy documents.“, based upon the "ISO/IEC 22989:2022 Information technology - Artificial intelligence - Artificial intelligence concepts and terminology” and “ISO/IEC 38507:2022 Information technology - Governance of IT - Governance implications of the use of artificial intelligence by organizations“, which have already been made public this year with consensus in many countries, including the US national body as SC 42.

The “ISO/IEC DIS 42001 Information technology - Artificial intelligence - Management system”, which is currently under development and is expected to be subject to audit in the future, also refer to the aforementioned international standards.

Public Comment #2:

INTEROPERABILITY

Comment:

AI Risk Management Framework FAQs include:

Q: 7. Why is a separate risk management framework for AI needed? There already are plenty of frameworks out there produced by NIST and others to address various related issues such as cybersecurity, privacy, and enterprise risk management?

A: Stakeholders are being asked to provide input to help determine whether it makes sense to relate the AI RMF to other NIST frameworks.

We believe that the NIST AI RMF is intended to consider the potential impact on individuals, groups, organizations, and society, and is closely related to the NIST Cybersecurity Framework and the NIST Privacy Framework.

NIST AIRMF and interoperability with them is not a uniform requirement, which varies by domain and company, but AI and cybersecurity in particular are closely related from a technical perspective.

Research on threat scenarios against AI systems that exploit AI-specific vulnerabilities is ongoing, and that there is a high level of interest in AI security in organizations.

To that end, we believe that at least a playbook should be added with reference information on the Severability of both standards, such as the strong relationship and correlation with this part of cybersecurity shown by NIST, so that AI and security professionals in the enterprise can easily work together.

The NIST SP800 series of standards, is also very user-friendly with references to ISO/IEC standards.

Public Comment #3:

Future use extension of AI RMF

Comment:

AI research and development, as well as the standards landscape, is evolving rapidly.

In the future, NIST AIRMF, as one of the core RMFs for digital advanced technologies, may be expanded to various fields of

use, for example, the following scenarios may be envisioned. Please tell us how NIST is currently considering future use extension of the AI RMF from a standardization perspective.

1) NIST has proposed the use of the AI RMF for voluntary use, and there has been strong interest in the private and public sectors for this type of resource. For example, in conjunction with U.S. legislation, it is envisioned that elements of soft law guidance could be applied to hard law guidance and used in the algorithm impact assessment process or by the FTC (Federal Trade Commission) to assess the impact of AI systems, etc.

2) In the future, it is also possible that AI RMF compliance, including internal audits and third-party certification systems, will be required as a condition of doing business, or that certain industry sectors will mandate compliance with the AI RMF. Also we believe that access to AI computing resources should not be restricted to only those organizations that comply with the AI RMF, creating a disparity of opportunity.

Public Comment #4:

Documentation

Comment:

The scope of documentation required by AIRMF is broad, but excessive documentation may run counter to the objectives and cause risk management and its underlying management system to become a skeleton. In addition, the appropriate scope of documentation for AI-specific algorithms and data, in particular, may cause a significant operational burden, including the cost of modification of enterprise risk management, including corporate project management, and the IT systems that support such management, and thus requires continued careful discussion.

Public Comment #5:

Further participation and collaboration

Comment:

“The AI Resource Center is expected to include a standards hub and a metrics hub, along with a terminology knowledge base and relevant technical and policy documents” it states.

We appreciate the NIST Trustworthy and Responsible AI Resource Center soliciting additional guidance, including a proposed AI RMF crosswalk with other resources – including standards and frameworks.

In order to further enhance the completeness of AIRMF, we look forward to further participation and collaboration in bottom-up discussions on the future positioning of AIRMF as a scenario from the perspective of standardization, envisioning transformations that should be open and continue to be made.

Respectfully submitted,

(General Lead of the committee)

Roy Sugimura, PhD, Supervisory Innovation Coordinator
Research Promotion Division for Artificial Intelligence of Information Technology and Human Factors,
National Institute of Advanced Industrial Science and Technology

(Lead for Proposal)
Hiromu (Kit) Kitamura, Evangelist (Artificial Intelligence/QMS/Legal)
Environment and Total Quality Management Department, NEC Corporation

(Experts contributed)
Yonosuke Harada (Institute of Information Security)
Toshihiro Suzuki (Oracle Japan)

CC) Information Technology Standards Commission of Japan