BlackBerry

September 28, 2022

National Institute of Standards and Technology
100 Bureau Drive
Gaithersburg, MD 20899

Re: AI Risk Management Framework: Second Draft

Dear NIST,

BlackBerry appreciates the opportunity to provide feedback on the second draft of the AI Risk Management Framework (RMF or "Framework"). We commend NIST leadership in the effort to develop the Framework and Playbook, and to establish NIST Trustworthy and Responsible AI Resource Center. We believe the outcome will substantially help the Framework users understand the context, and identify and manage significant risks of their AI systems in an effective and flexible manner.

For nearly 40 years, BlackBerry has invented, created, and built security solutions to give people and businesses the ability to stay secure, mobile and productive. Today, BlackBerry continues to place trusted security protection everywhere. Our software is present in over 500 million endpoints including automobiles, mobile phones, laptops and IoT devices. We deploy next-generation cybersecurity protection, detection and response, leveraging the most advanced artificial intelligence and machine learning technologies in our Cylance AI platform.

As explained in detail below, our comments cover general aspects of the Framework, each function (i.e., Govern, Map, Measure and Manage). In summary, we recommend NIST continue to do the following:

- Develop guidance for context-specific tailoring of categories and subcategories;
- Harmonize the Framework with relevant standardization activities of other organizations to increase the global relevance of the Framework; and
- Extend the Framework coverage for each trustworthiness characteristic.

1. General comments

Tailoring

BlackBerry agrees that Framework users may apply the Framework functions as best suits their needs for managing AI risks and some organizations may choose to select from among the categories and subcategories (Page 18). In addition, we highlight the need for tailoring the categories and subcategories to manage the AI risks unique to the context of their intended use of AI systems. We suggest NIST develop additional guidance and resources for supporting tailoring activities in the Framework and Playbook.

BlackBerry Corporation
3001 Bishop Drive, Suite 400, San Ramon, California, 94583 USA. tel: +1 (925) 242-5660 fax: +1 (925) 242-5661

Harmonization

BlackBerry appreciates NIST's efforts to ensure the Framework is consistent or aligned with other existing or ongoing approaches to AI risk management, by incorporating definitions from the OECD Framework for the Classification of AI Systems and relevant ISO/IEC technical specifications. We encourage NIST to continue the harmonization of the Framework with other global and regional evolving standardization work, including ISO, IEC, IEEE and CEN/CELEC. Considering our globally interconnected economy, a globally harmonized standard reflecting U.S. interests would strengthen the nation's AI leadership while benefiting the Framework's users.

Safety

The Framework captures challenges for AI risk management and states that the AI RMF equips organizations to define reasonable risk tolerance, manage those risks, and document their risk management process in Section 3.2. We would note there are domain-specific standards to address such challenges, setting risk tolerance, measuring and prioritizing risks -- for example, ISO 21448:2022 "Road vehicles – Safety of the intended functionalities" (SOTIF). We encourage NIST to ensure the Framework remains consistent with and takes advantage of already developed standards or best practices.

NIST Trustworthy and Responsible AI Resource Center

BlackBerry supports the intent to develop an AI Resource Center that receives contributions from a broad community and functions as a hub of knowledge and resources supporting the implementation of the Framework. While we appreciate the suggested topics for contributions (listed in Page iii of the draft), additional guidance can address not only the security concerns but also those with other AI trustworthiness characteristics including bias, privacy and safety.

Stakeholders

The Framework frequently refers to stakeholders without defining them. In some cases, the Framework refers to its users as stakeholders; in other cases, the stakeholders are external to AI actors engaging in AI system development. BlackBerry suggests NIST define the term "stakeholders" and clarify the scope of stakeholders in the description of categories and subcategories, to the extent possible.

2. Govern function

Roles of operations and users

The AI lifecycle includes development, deployment, operation and decommissioning. Operations and end users play important roles in AI risk management, monitoring and identifying known and emergent risks. BlackBerry believes that the operations and end user perspective should be emphasized in actions in the Playbook for certain subcategories as they contribute to AI risk

management. For example, the actions for Govern 2.1 within the Playbook can add operations and end user roles and responsibilities.

Feedback from end users and domain experts

BlackBerry agrees with NIST that it is essential to collect, consider, prioritize, and integrate external stakeholder's feedback regarding the potential individual and societal impacts related to AI risks (Govern 5.1). We note that the description of the subcategory in the Playbook focuses on participatory stakeholder engagement. While wide-ranging stakeholder involvement is important to identify AI risks to individuals or a group that can be affected, we would highlight the importance of the Framework users collecting and evaluating the feedback or data from the end users and domain experts to identify emergent scenarios and risks that can cause harm to humans in certain AI applications.

3. Map function

Negative impacts and risks

The Framework lists organizations' activities (Page 21) that reflect broad perspectives from diverse internal teams and engagement with external stakeholders pursuing proactive risk prevention and trustworthy AI system development. In addition to the activities listed, BlackBerry would highlight the importance of proactively identifying known and foreseeable negative impacts related to the intended use of the AI system based on the broad perspectives obtained.

Stakeholder selection

BlackBerry agrees with the importance of engaging a broad set of stakeholders to improve the capacity of AI actors to assess system impacts – and subsequently – system risks, as described in the Playbook (Map 3.2). We would note that the breadth and depth of stakeholder involvement depends on the context and intended use of AI systems, as specific domain expert knowledge is imperative for high-risk use cases. In this regard, the primary factor determining the types and number of stakeholders is the context of the intended use of the AI systems, not organizations (Map 1.6 in the Playbook).

Context relevant trustworthiness

The Measure function relies on the outcome of the Map function to identify context-relevant measures of trustworthiness. However, the description of the Map function, categories and subcategories currently offers little discussion on risks in terms of trustworthiness characteristics specific to the context. BlackBerry requests that NIST elaborate on how the Map function can help organizations identify the most and least relevant trustworthiness characteristics based on the contextual assessment. Doing so could assist organizations in explaining and documenting why certain risks or trustworthiness characteristics are not being measured (Measure 1.1). We think design decisions (Map 1.7) should consider not only socio-technical implications but other implications on AI trustworthiness characteristics as well.

BlackBerry Corporation
3001 Bishop Drive, Suite 400, San Ramon, California, 94583 USA. tel: +1 (925) 242-5660 fax: +1 (925) 242-5661

4. Measure function

Tools

Tools play key roles for test, evaluation, verification, and validation throughout the AI life cycle, and measuring context-relevant risks or trustworthiness characteristics. In particular, the Framework and the Manage function rely on the correctness of tools (e.g., minimized erroneous outputs and failures in detecting errors) and the proper usage of tools. BlackBerry suggests that NIST develop guidance on the required level of confidence for AI tools to reliably support the Framework execution.

Safety

The subcategory, Measure 2.5, provides that the deployed product is demonstrated to be safe and can fail safely and gracefully if it is made to operate beyond its knowledge limits. BlackBerry would note that rigorous evaluation is required to demonstrate that residual risk from unknown hazardous scenarios meets the acceptance criteria with sufficient confidence to achieve the outcome. The safety metrics need to be extended to cover the breadth and depth of validation.

Feedback about measurement efficacy

We note that not only improvement but degradation in performance measurement should be identified and documented (Measure 4.3). For effective measurement, AI actors in development and operations should identify field data which can indicate context-relevant risks and trustworthiness characteristics, and integrate mechanisms for collecting them from the AI systems or end users in AI system implementation or operations.

5. Manage function

AI lifecycle

The subcategory, Manage 1.1 provides that a determination be made as to whether the AI system achieves its intended purpose and stated objectives and should proceed in development or deployment. We propose to add decommissioning of the AI system as the determination is applicable to the last phase of AI lifecycle.

Risk based prioritization

The subcategory, Manage 1.2 states that treatment of documented risks is prioritized based on impact, likelihood, and available resources methods. BlackBerry notes that in certain cases, the likelihood cannot be determined confidently, and the available resources are less relevant than the other factors. We propose to change “impact, likelihood, and available resources” to “impact, likelihood, or available resources”.

BlackBerry Corporation
3001 Bishop Drive, Suite 400, San Ramon, California, 94583 USA. tel: +1 (925) 242-5660 fax: +1 (925) 242-5661

6. Summary

BlackBerry supports NIST leadership in the effort to develop the Framework and Playbook, and to establish the Trustworthy and Responsible AI Resource Center. We believe the outcome will significantly help Framework users understand the context, identify and manage risks of their AI systems in an effective and flexible manner. Mr. Takashi Suzuki (tsuzuki@blackberry.com) is available to respond to any questions concerning BlackBerry's response.

Respectfully submitted,

Takashi Suzuki

Takashi Suzuki
Senior Director, Standards

BlackBerry Corporation
3001 Bishop Drive, Suite 400, San Ramon, California, 94583 USA. tel: +1 (925) 242-5660 fax: +1 (925) 242-5661