PUBLIC SUBMISSION

As of: 8/20/21 11:23 AM
Received: August 19, 2021
Status: Pending_Post
Tracking No. ksj-e3r5-zgop
Comments Due: August 19, 2021
Submission Type: Web

Docket: NIST-2021-0004
Artificial Intelligence Risk Management Framework

Comment On: NIST-2021-0004-0001
Artificial Intelligence Risk Management Framework

Document: NIST-2021-0004-DRAFT-0035
Comment on FR Doc # 2021-16176

Submitter Information

Email:
Organization: Rotunda Solutions

General Comment

Artificial Intelligence (AI) is not only advancing fast, but it has also been a rapidly accepted technology that is currently being utilized throughout various industries to increase effectiveness, understand processes, provide insight, and alleviate burden from workers in order to allow them to focus on higher cognitive loading tasks. However, regulatory and security understanding has not kept up with this advance in technology and therefore has not changed to incorporate fairness, security, explainability, or proper reporting measures into the development and usage of these tools. Therefore it is with great pleasure that I respond to this RFI as the Principal Researcher of Rotunda Solutions, Inc, so that we may provide our understanding of this field into this very important work.

Rotunda Solutions is a Systems Engineering and Data Analytics firm with clients throughout the Federal Government, as well as the commerical, academic, and non-profit sectors. Rotunda provides consulting services to these entities and regularly engages with its academic and industrial colleagues through publication, conference presentation and attendance, and assistance in the development of policy related to these fields. A key pillar of the Rotunda Analytics and Innovation Lab (RAIL)—the research wing of Rotunda Solutions—revolves around AI security and fairness. In addition, Rotunda prides itself on the usage, research, and development of explainable AI technologies, as well as its ability to explain these technologies to both technical and non-technical audiences. Pertaining to this RFI, employees of Rotunda Solutions have actively served on various efforts with clientle, research, and policy regarding AI security, fairness, and ethics.

The development of a Risk Mitigation Framework (RMF) must consider methodologies which incorporate current industrial and academic understanding of security vulernabilites and mitigation techniques, inherent bias and fairness concerns, ethical considerations, and the ability to understand how a particular tool arrived at its conclusion. This includes not only the development of the algorithms and models themselves, but also the collection, storage, transfer, and sharing of datasets utilized to develop such technologies. Current efforts at Rotunda Solutions are focused on the research and development of methodologies within fields of AI Security in order to provide users with the ability to understand not only the vulnerability of their assets to various adversarial attacks, but also to understand the origin of these vulnerabilities and how to mitigate their affect without degrading the effectiveness of developed AI techniques. This is a core area in which effort must be focused: how can AI be made secure, explainable, and fair, while remaining effective. These areas can often be seen in competition. Often, the more secure an AI tool becomes, the less effective it can be. In addition, fairer tools tend to be more complex whether through extensive data collection or extensive model development. The construction of an RMF which encorporates such a fast-paced technology can only be done through consensus and the ability for evolution of the RMF as the technology advances.