As of: 8/19/21 8:59 AM
Received: August 18, 2021
Status: Pending_Post
Tracking No. ksi-crwf-hr0k
Comments Due: August 19, 2021
Submission Type: Web

PUBLIC SUBMISSION

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-0022
Comment on FR Doc # 2021-16176

Submitter Information

Email:
Organization: AI Village

General Comment

The AI Village* welcomes the NIST RFI on Artificial Intelligence Risk Management Framework. Such a framework is long overdue to confidently adopt AI in production systems, including mission-, security- and safety-critical applications.
Our response is articulated on five axes: (i) concrete and current risk, (ii) actionability, (iii) organizations focus, (iv) case specific and (v) existing and upcoming standards.

More specifically each of those five axes tries to answer a specific need of the framework:

Concrete and current risk: This addresses the lack of adequate and easily manipulable risk definition in the case of AI systems and the current divide between risks faced today in production by organizations and the hypothetical and future risks considered in a number of Reliable AI academic publications. As a strongly industry focused organization, we believe the former should be given immediate priority and the latter should be used primarily as a support vector for threat anticipation.

Actionability: This axis addresses the current difficulty in making AI risk assessments and mitigation operational including both the methodological and tooling gaps in conducting end-to-end AI risk assessments. We identify gaps in enforceability as well as current risk and testing methodologies that will need to be filled ahead of proper AI risk assessment engagements.

Organizational focus: By this axis we address the incentives, budget obtention, team reorganizations, business integration and related organizational challenges that implementers will eventually face in their respective organizations. The framework will need to provide answers on those points to ease its deployment in complex governance schemes.

Case specific: By this axis we seek to address specific challenges that will arise on a case by case basis and which a generic framework might be incapable of covering. In our response, we take specific attention in addressing both large and small organizations, specific industries like finance, ICS and pharmaceuticals etc.

Existing and upcoming standards: Our submission draws heavily from a number of existing and upcoming security, privacy and AI regulations that are listed in appendix A. We curated this list based on their relevance and implementation likelihood in target organizations. The upcoming AI Risk framework should tightly integrate with those to limit conflicts and necessary additional work, thereby facilitating adoption.

Our full response is included in separate file.

*The AI Village is a community of hackers and data scientists working to educate the world on the use and abuse of artificial intelligence in security and privacy. We are academics, IT specialists, security experts, students, philosophers, and concerned citizens.

Attachments

AIV NIST RMF Response