PUBLIC SUBMISSION

As of: 9/16/21 10:08 AM
Received: September 14, 2021
Status: Pending_Post
Tracking No. ktk-7cpe-ltbz
Comments Due: September 15, 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-0072
Comment on FR Doc # 2021-16176

Submitter Information

Name: Eugene Neelou Alex Polyakov, Adversa AI
Address: United States,
Email:

General Comment

Comments are provided by Eugene Neelou and Alex Polyakov, experts in cybersecurity, artificial intelligence, and risk management. Both are founders of Adversa.AI, a world-class Israeli startup on a mission to increase trust in AI systems.

Recently, Adversa.AI has released the unique report called “The Road to Secure and Trusted AI: The Decade of AI Security Challenges” that demonstrates the progress toward AI trustworthiness over the past 10 years across academia, government, and industry.

Besides many insights and infographics, the Adversa Report has introduced 2 essential resources for the development of the AI Risk Management Framework:
1. The Map of Trustworthy AI covers all principles and requirements for trusted AI.
2. The Lifecycle for Secure AI describes activities for all security stages for AI systems.

Please find our comments first and the mentioned resources in the end.

Attachments

Adversa-Comments-for-NIST-AI-Risk-Management-Framework