Reply

RFI Response to 84 FR 18490 from the AI Security Alliance

You replied on Mon 6/10/2019 1:25 PM

KR

Kapil Raina <kapil@aisecurityalliance.org>
Mon 6/10/2019 1:21 PM
ai_standards; Kapil Raina <kapil@aisecurityalliance.org>

To Whom It May Concern:

The AI Security Alliance (www.aisecurityalliance.org) appreciates the opportunity to provide input to the NIST RFI cited as 84 FR 18490.

As background, the AI Security Alliance is an industry organization that seeks to provide guidance and influence the security of the use of artificial intelligence. In that regard, our membership and interests span across government, academic, and commercial applications and concerns.

The promise of AI has immense benefits across all applications that affect citizens and organizations alike. In our response, we ask NIST to consider some challenges we see - especially as many standards technical or legal are still very immature to guide both vendors and consumers of AI systems. When considering concerns around AI, this comment seeks to address three key areas: security, privacy, and transparency. While we seek to highlight challenges, we do not present explicit solutions in this response. In both our working groups and in the commercial markets, there are a number of efforts underway to attempt to solve these challenges.

Finally, in this response, as it does not relate directly to security and privacy, we do not address here a key area of concern for citizens - bias (of any type, including race, gender, etc..). We hope that NIST will also consider bias as part of its analysis of AI and its applications to ensure an equitable and transparent impact on the citizenry.

Key Elements of an AI System