PUBLIC SUBMISSION

As of: 8/6/21 12:54 PM
Received: August 06, 2021
Status: Pending_Post
Tracking No. ks0-hs6w-uc1l
Comments Due: August 19, 2021
Submission Type: API

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-0004
Comment on FR Doc # 2021-16176

Submitter Information

Name: Anonymous Anonymous
Email: default@yahoo.com

General Comment

In respect to the current topics. Perhaps consider these as additional or enhance where noted;
- Require explanations of how AI works with any systems capable of handling personal or private information, including integrations with such systems (incorporate in item 8 or 12 ?)
- Require assurances that AI systems are protected against unauthorized access and manipulation (incorporate in item 2)
- Considerations for threat intelligence incorporated to identify and address new and emerging threats to AI (incorporate in item in 4)
- Require auditable designs and human oversight to identify AI system compromises with appropriate response handling. AI assessments, pre-deployment. product certification (incorporate in item 3)
- Regulatory interpretation of relevant regulations relating to AI systems produced data, including all data privacy (maybe incorporate in item 6?)
- Preventive measures defined to address adversaries potential to cause machine learning and AI models to misinterpret inputs into the systems to behave in a way to the advantage of an attacker. (incorporate in item in 2, maybe 8 too)
- Describe staffing requirements for AI development, management, and support to include education, certification , and to sustain subject matter accreditation (maybe covered already in 11)