PUBLIC SUBMISSION

As of: 8/10/21 8:46 AM
Received: August 09, 2021
Status: Pending_Post
Tracking No. ks5-ak7o-nmza
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-0005
Comment on FR Doc # 2021-16176

Submitter Information

Name: Anonymous Anonymous

General Comment

NIST is requesting information related to the following topics:
1. The greatest challenges in improving how AI actors manage AI-related risks—where "manage" means identify, assess, prioritize, respond to, or communicate those risks;
*Voluntary Participation and Reporting is likely insufficient. Mandatory reporting must be required.

2. How organizations currently define and manage characteristics of AI trustworthiness and whether there are important characteristics which should be considered in the Framework besides: Accuracy, explainability and interpretability, reliability, privacy, robustness, safety, security (resilience), and mitigation of harmful bias, or harmful outcomes from misuse of the AI;
*A Complete Standard for Hazard Identification and Mitigation, Threat Identification and Risk, and Specific Scoped Vulnerability must be created and maintained for all eternity.

3. How organizations currently define and manage principles of AI trustworthiness and whether there are important principles which should be considered in the Framework besides: Transparency, fairness, and accountability;
*Project Motivation and Specific, Issue-Based, Moral Value Statements with Proof-of-No-Conflict documents must be recorded.

4. The extent to which AI risks are incorporated into different organizations' overarching enterprise risk management—including, but not limited to, the management of risks related to cybersecurity, privacy, and safety;
*At last, Enterprise must formally be welcomed into the fold of Managed Risk, just as Infrastructure and others have before it. There are classifications, Tiers, and Strategies.

5. Standards, frameworks, models, methodologies, tools, guidelines and best practices, and principles to identify, assess, prioritize, mitigate, or communicate AI risk and whether any currently meet the minimum attributes described above;
*Start with the basic inclusions of RAMCAP, and work your way out.

6. How current regulatory or regulatory reporting requirements (e.g., local, state, national, international) relate to the use of AI standards, frameworks, models, methodologies, tools, guidelines and best practices, and principles;
*I envision something like the current practices of Building Planning, with the ongoing practices of Emissions Monitoring, with similar penalties and practices.

7. AI risk management standards, frameworks, models, methodologies, tools, guidelines and best practices, principles, and practices which NIST should consider to ensure that the AI RMF aligns with and supports other efforts;
*Existing Hazard, Threat, Risk, Vulnerability and Resource-Use Planning methods should be used and expanded upon.

8. How organizations take into account benefits and issues related to inclusiveness in AI design, development, use and evaluation—and how AI design and development may be carried out in a way that reduces or manages the risk of potential negative impact on individuals, groups, and society.
*Once again, Mandatory reporting of project Motivations into the public record, with customer/stakeholder accountability from the project owners, is the best and only perceived way.

9. The appropriateness of the attributes NIST has developed for the AI Risk Management Framework. (See above, "AI RMF Development and Attributes");
10. Effective ways to structure the Framework to achieve the desired goals, including, but not limited to, integrating AI risk management processes with organizational processes for developing products and services for better outcomes in terms of trustworthiness and management of AI risks. Respondents are asked to identify any current models which would be effective. These could include—but are not limited to—the NIST Cybersecurity Framework or Privacy Framework, which focus on outcomes, functions, categories and subcategories and also offer options for developing profiles reflecting current and desired approaches as well as tiers to describe degree of framework implementation; and
*Understanding the existence of AI Agents/Entities as primarily a "Risk to be Reduced with Untold Benefits" drives the contriving of a Risk-Mitigation-First Framework. (please see my attached comments)

11. How the Framework could be developed to advance the recruitment, hiring, development, and retention of a knowledgeable and skilled workforce necessary to perform AI-related functions within organizations.
*(please see my attached comments)

12. The extent to which the Framework should include governance issues, including but not limited to make up of design and development teams, monitoring and evaluation, and grievance and redress."
*(please see my attached comments)

Attachments

comments2