Elham Tabassi
July 11, 2024

Grateful for the invitation and delighted to be here.

NIST is a non-regulatory agency under Dept of Commerce, with a unique mission—to advance U.S. innovation and industrial competitiveness—

NIST has a broad portfolio of research and a long tradition of cultivating trust in technology. We do that by advancing measurement science and standards - measurement science and standards that makes technology more reliable, secure, private, fair, - and that is what we are doing in AI space.

NIST was established in 1901 to "fix the standard of weights and measures," – our predecessors created and advanced standards to measure basic things, like length and mass, temperature and time, light and electricity — essential for technological innovation and competitiveness at the turn of the 20th century. We are following the same course: working with and engaging the community in figuring out proper standards for advanced technologies of our time, like AI.

A little over a year ago we released the NIST AI Risk Management Framework or AI RMF –

- Directed by a congressional mandate, AI RMF is a voluntary framework for managing the risk of AI in a flexible, structured, and measurable way. It was developed in close collaboration with AI community, engaging diverse groups of different background, expertise, and perspectives. The Framework is intended to be voluntary, rights-preserving, non-sector-specific, and use-case agnostic, providing flexibility to organizations of all sizes and in all

sectors and throughout society to implement the approaches in the Framework.

- In March we released AI resource center as a one stop shop of knowledge, data, tools for AI risk management. It has AI RMF and its playbook in an interactive, searchable, filterable manner.
    - This resource center is certainly a work in progress and stays a work in progress. We like to add additional capabilities like standards hub or repository of metrics and more.
- In June, we put together a Generative AI Public Working Group where more than 2000 volunteers helped us to study and understand the risks of Generative AI.
- Our latest assignment, Executive Order on safe, secure and trustworthy AI builds upon the foundational work we have been doing in AI.
- Specifically, the EO directed NIST to: develop evaluation, red-teaming, safety, and cybersecurity guidelines; facilitate development of consensus-based standards; and provide testing environments for evaluation of AI systems. These guidelines and infrastructure will be a voluntary resource to be used by the AI community for trustworthy development and responsible use of AI.

AI is one of most transformative technologies of our time. One with tremendous opportunity to improve our lives, but also one that comes with its negative consequences and harms. When it comes to AI, there is a lot less we know that we should. We should change that.

1. We must engage in efforts to advance our scientific understanding of the limits and capabilities of these powerful AI models and their behaviors.

2. We must address AI's impact on people and society and plant through technical, social and sociotechnical lenses

3. We should advance research on identifying, measuring, managing and mitigating risks including safety, security, privacy, reliability, interpretability

4. We must actively seek and incorporating insights from a diverse range of experts representing diverse set of backgrounds and perspectives.

5. We must also cultivate and strengthen international collaborations and cooperation on AI issues

Bottom line is that we want technologies that works accurately and reliably. Technologies that is easy to do the right thing, difficult to do the wrong thing and easy to recover if and when it goes off course.

Standards play a crucial role in achieving that and for the development and adoption of new and emerging technologies.

Standards set consistent "rules of the road" and are critical to enable market competition, preclude barriers to trade, and allow innovation to flourish.

Standards are especially important in the field of AI, where policymakers and regulators in the United States and abroad are looking to the standards ecosystem to guide AI actors on how to implement high-level principles and policies. In its role as federal AI standards coordinator, NIST works across the government and with industry stakeholders to identify critical standards development activities, strategies, and gaps.

By fostering dialogue and collaboration among stakeholders, we can accelerate the research, trustworthy development and responsible use of AI in ways that maximizes its potential for benefits and minimizes its harm or negative consequences

Together we are helping build the scientific foundation necessary to ultimately understand, shape, and collectively benefit from how AI can and will transform our society.

we recognize the road ahead is long and full of challenges and opportunities. I started by saying that When it comes to AI, there is a lot less we know that we should. The operative word there is “we”. We can and should work together to change that. Thanks for your thoughtful leadership, engagement, and collaborations.