

NIST AI Program

Elham Tabassi
Information Technology Laboratory
August 8, 2019

Federal Engagement in Artificial Intelligence Standards

EXECUTIVE ORDERS

Executive Order on Maintaining American Leadership in Artificial Intelligence

— INFRASTRUCTURE & TECHNOLOGY | Issued on: February 11, 2019



Within 180 days...

Secretary of Commerce, through Director of NIST, shall issue a plan for Federal engagement in the development of technical standards and related tools in support of reliable, robust, and trustworthy systems that use AI technologies.

Our Approach

“NIST’s efforts will support the development of standards for AI that reflect federal priorities for innovation, public trust and confidence.”



Request for information, May 1 – June 10, 2019.



Workshop May 30, 2019.



Draft Plan for public comment, July 2-19, 2019.

Request For Information



Topic Area 1

What's out there already? What's in the works?

current status and plans



Topic Area 2

What do we really need the most that we don't yet have?

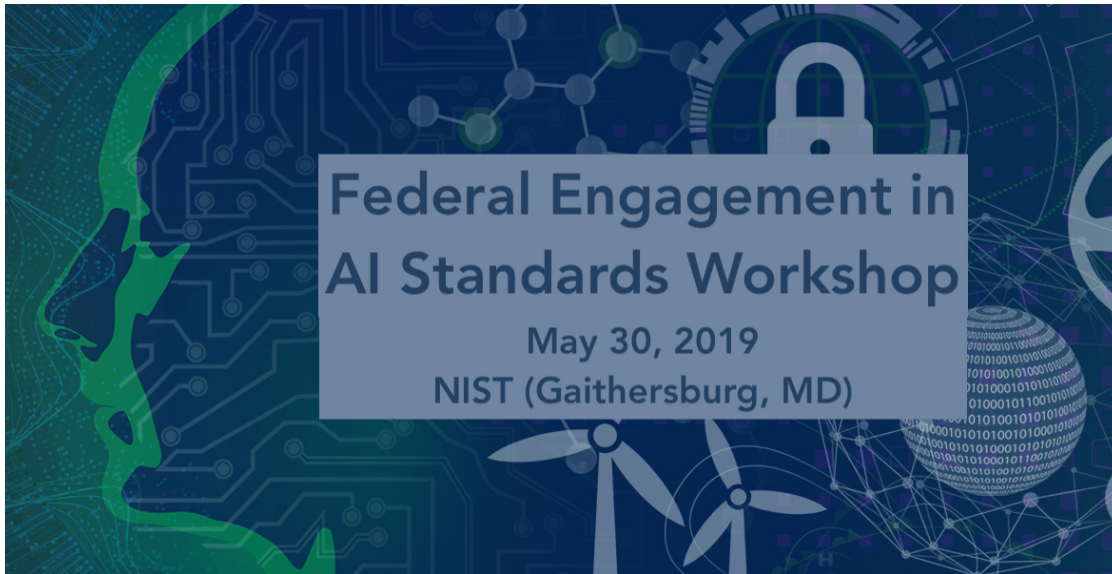
needs and challenges



Topic Area 3

What can and should the federal government do first and foremost?

role of federal agencies



Purpose

Engage private and public sector organizations and individuals



Outcome

Outline of a plan

By Numbers



97

RFI
RESPONSES



>400

WORKSHOP
ATTENDEES



6

BREAKOUT
SESSIONS



43

PUBLIC
COMMENTS



2

DOCUMENTS



2

DAYS TILL
DEADLINE

**U.S. LEADERSHIP IN AI:
A PLAN FOR FEDERAL ENGAGEMENT IN
DEVELOPING TECHNICAL STANDARDS
AND RELATED TOOLS**

DRAFT FOR PUBLIC COMMENT



**Comment period
July 2 – 19, 2019**



**3 Sections
6 Appendices**

**PREPARED IN RESPONSE TO EXECUTIVE ORDER 13859
SUBMITTED ON AUGUST XX, 2019**

Structure of the Plan



AI and Standards

What AI technical standards and related tools are needed?

needs and challenges



Priorities

What's the appropriate level and type of involvement?

USG AI standards



Recommendations

What can and should the federal government do first and foremost?

federal engagement

1 Standards and Artificial Intelligence

Risk Management **Safety**
Performance Testing Methodology
Human Interaction Societal & Ethical
Trustworthiness Consideration
Data and Networking Privacy
Knowledge **Metrics** Governance
Concepts and Terminology



Technically sound, fit for purpose, and timely AI standards.

2 U.S. Government AI Standards Priorities



www.nist.gov/topics/artificial-intelligence/ai-standards

1. Which standards development efforts merit federal engagement?

2. Which standards characteristics are important?

3. Levels of U.S. Government engagement in AI standards

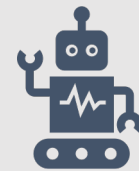
4. Practical steps for federal engagement in AI standards

3 Draft Recommended Actions



Coordination

Bolster AI standards-related knowledge, leadership, and coordination among Federal agencies to maximize effectiveness and efficiency.



Research

Promote focused research to accelerate broader exploration and understanding of how aspects of trustworthiness can be practically incorporated within standards.



Partnership

Support and expand public-private partnerships to develop and use AI standards and related tools to advance trustworthy AI.



Engagement

Strategically engage with international parties to advance AI standards for U.S. economic and national security needs.

1 Definitions

2 AI Standards

3 Related Tools
for AI Standards

4 Assignment
and Approach

5 Request for
Information

6 Workshop
Agenda



U.S. LEADERSHIP IN AI:

A Plan for Federal Engagement in Developing
Technical Standards and Related Tools

Prepared in response to Executive Order 13859
Submitted on August XX, 2019

Trustworthy AI

Trustworthy AI



accurate



secure



robust



explainable



objective



reliable

and more ...

Terminology and Taxonomy of attacks and defenses for Adversarial Machine Learning.



Collaboration with MITRE.



Extensive literature survey.



Draft for public comment planned for September 2019.

Explainable AI

Forms the bases of addressing fairness, bias, transparency, security, safety and ultimately trust in AI systems.



Developed principles of explainable AI.



Socialize with experts in the community.



Draft for public comment planned for January 2020.



QUESTIONS?

STAY IN TOUCH

ai_standards@nist.gov

www.nist.gov/topics/artificial-intelligence/ai-standards