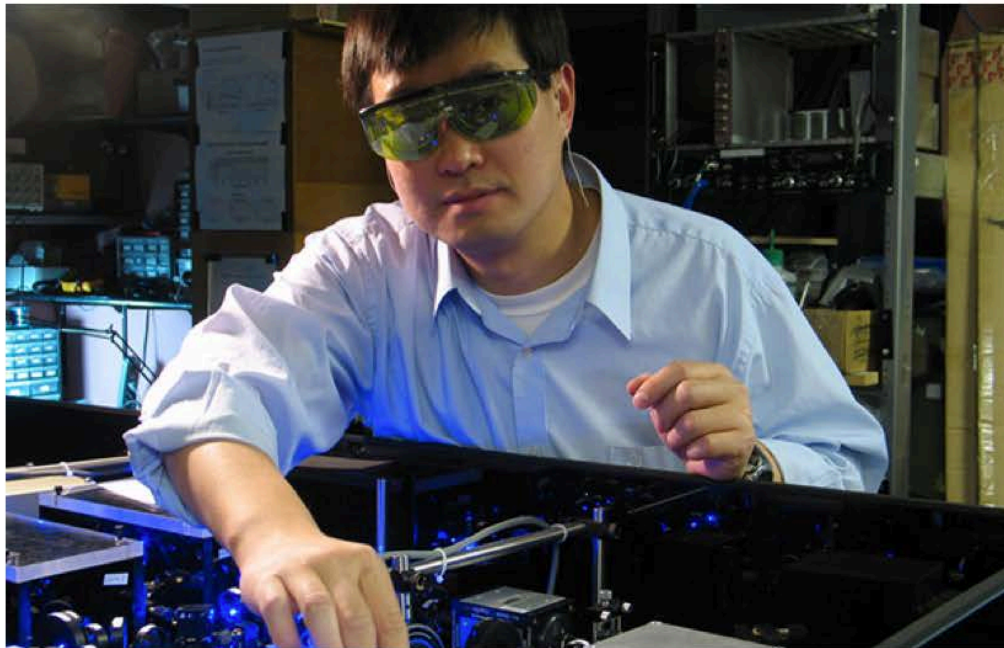


# NIST AI Activities

## Chuck Romine

### June 4, 2019

# Cultivating Trust in IT and Metrology



# ITL's work

Fundamental  
Research

Applied  
Research

Standards +  
Best Practice  
Guides

Adoption

Image Credit: wsj.com

# Fundamental and Applied Research and Standards for AI Technologies (FARSAIT)



## Applied

Catalyzing the use of machine learning and AI within NIST scientific program.

## Fundamental

Measure and enhance the security and trustworthiness of AI systems.

*Office of Science and Technology Policy*

# NSTC



**MLAI Subcommittee**  
**Chaired by NIST, OSTP, DoE**

Networking and Information  
Technology Research and  
Development (NITRD) AI  
Interagency Working Group

**AI Select Committee**  
**Chaired by OSTP, NSF, DARPA**

# Trustworthy AI

accuracy

reliability

privacy

robustness

explainability



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.



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.

# Federal Engagement in Artificial Intelligence Standards Workshop

# Executive Order on Maintaining American Leadership in AI

EXECUTIVE ORDERS

## Executive Order on Maintaining American Leadership in Artificial Intelligence

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



[www.whitehouse.gov/presidential-actions/executive-order-maintaining-american-leadership-artificial-intelligence/](https://www.whitehouse.gov/presidential-actions/executive-order-maintaining-american-leadership-artificial-intelligence/)



Within 180 days of the date of this order,

NIST is tasked with developing 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 and timetable

“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, 2019. Closes on June 10, 2019.



Workshop on May 30, 2019.



Draft Plan for public comment, late June.

# 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**

# Federal Engagement in Artificial Intelligence Standards Workshop



[www.nist.gov/topics/artificial-intelligence/ai-standards](http://www.nist.gov/topics/artificial-intelligence/ai-standards)



## Purpose

Engage private and public sector organizations and individuals in discussions that advance the development of a plan for Federal engagement in AI standards.



## Outcome

Annotated outline of a plan for Federal engagement in the development of technical standards and related tools



## Panel Session (am)

What's next in standards setting for AI



## Panel Session (pm)

What AI standards are needed by Federal government agencies?



## Breakout Session (am)

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



## Breakout Session (pm)

How should the Federal government engage?

# Draft outline

Draft Outline for the AI Standards Federal Engagement Plan (24-May-19)

A Plan for Federal Engagement in Developing Technical Standards and Related Tools Supporting Reliable, Robust, and Trustworthy Systems that Use AI Technologies

## 1. The Assignment and Approach

Executive Order (EO 13859) Maintaining American Leadership in Artificial Intelligence, February 11, 2019

Outreach and Consultation

- Publication of a Request for Information in the Federal Register
- Contacts and discussions with Federal agencies
- Workshop on a Federal AI standards engagement strategy
- Public review and comment on a draft AI standards Federal engagement plan

## 2. Criteria and Priorities for U.S. Government Engagement in AI Standards and Related Tools

Topic: Standards as a Technical and Policy Tool

Topic: Federal Engagement Strategy

Topic: Engagement and Prioritization Criteria

## 3. Effective, Timely and Robust AI Standards: A Vision for the Future

Topic: AI Standards and the Standards Setting World

Topic: Defining AI Standards and Related Tools for this Plan

Topic: Establishing Characteristics of Trustworthy AI

## 4. Existing and Planned AI Standards

Topic: What's Out there Already? What's in the Works?

Topic: How Should the Federal Government Engage?

## 5. Recommendations

Topic: Recommendations for USG Action

Topic: Recommendations for AI Community

### Appendices:

- I. Definitions
- II. EO
- III. RFI
- IV. Workshop Agenda
- V. AI Standards & Related Tools



May 30:

Discussed and annotated the outline.

Late June:

Draft for public comment.



# By Numbers



**217**  
WORKSHOP  
ATTENDEES



**>100**  
ENTITIES



**6**  
BREAKOUT  
SESSIONS



**34+**  
RFI  
RESPONSES



**2**  
DOCUMENTS



**67**  
DAYS TILL  
DEADLINE

# Moving forward



[www.nist.gov/topics/artificial-intelligence/ai-standards](http://www.nist.gov/topics/artificial-intelligence/ai-standards)

**1.** June 10: RFI closes.

**2.** June 19: Distribute draft Plan to federal agencies for review.

**3.** July 1: Distribute draft for public review.

**4.** July 30: Final report for clearance.



# STAY IN TOUCH

---

#NISTAIStandardsPlan  
[ai\\_standards@nist.gov](mailto:ai_standards@nist.gov)

[www.nist.gov/topics/artificial-intelligence/ai-standards](http://www.nist.gov/topics/artificial-intelligence/ai-standards)