

118TH CONGRESS
2D SESSION

H. R. 9466

To direct the National Institute of Standards and Technology to catalog and evaluate emerging practices and norms for communicating certain characteristics of artificial intelligence systems, including relating to transparency, robustness, resilience, security, safety, and usability, and for other purposes.

IN THE HOUSE OF REPRESENTATIVES

SEPTEMBER 6, 2024

Mr. BAIRD (for himself and Mr. LIEU) introduced the following bill; which was referred to the Committee on Science, Space, and Technology

A BILL

To direct the National Institute of Standards and Technology to catalog and evaluate emerging practices and norms for communicating certain characteristics of artificial intelligence systems, including relating to transparency, robustness, resilience, security, safety, and usability, and for other purposes.

1 *Be it enacted by the Senate and House of Representa-*
2 *tives of the United States of America in Congress assembled,*

3 **SECTION 1. SHORT TITLE.**

4 This Act may be cited as the “AI Development Prac-
5 tices Act of 2024”.

1 **SEC. 2. NIST RESEARCH ON DEVELOPMENT BEST PRAC-**
2 **TICES.**

3 Section 22A of the National Institute of Standards
4 and Technology Act (15 U.S.C. 278h–1) is amended—

5 (1) by redesignating subsection (h) as sub-
6 section (i); and

7 (2) by inserting after subsection (g) the fol-
8 lowing new subsection:

9 “(h) ASSESSMENT OF THE PRACTICES OF ARTIFI-
10 CIAL INTELLIGENCE DEVELOPMENT.—

11 “(1) IN GENERAL.—The Director of the Na-
12 tional Institute of Standards and Technology (in this
13 subsection referred to as the ‘Director’) shall, sub-
14 ject to the availability of appropriations, develop,
15 and periodically update, in collaboration with other
16 public and private sector organizations, voluntary
17 guidance for practices and guidelines relating to the
18 development, release, and assessment of artificial in-
19 telligence systems. Such guidelines shall satisfy the
20 following:

21 “(A) Define methods and guidelines for de-
22 veloping reasonable risk tolerances for various
23 use cases of artificial intelligence systems based
24 on the following:

25 “(i) The risks associated with the in-
26 tended and unintended applications, use

1 cases, and outcomes of the artificial intel-
2 ligence system at issue, based on the
3 guidelines specified in the voluntary risk
4 management framework for trustworthy
5 artificial intelligence systems, or successor
6 framework, authorized under subsection
7 (c), which may include different categories
8 of risk, such as the following:

9 “(I) Security risks, including
10 threats to national security.

11 “(II) Economic risks, including
12 threats to economic opportunities.

13 “(III) Social risks, including in-
14 fringement upon constitutional rights,
15 privileges, or liberties.

16 “(ii) Such other factors as the Direc-
17 tor determines appropriate and consistent
18 with this subsection.

19 “(B) Categorize and list practices and
20 norms for communicating relevant characteris-
21 tics, including robustness, resilience, security,
22 safety, fairness, privacy, validation, reliability,
23 accountability, and usability, of artificial intel-
24 ligence systems, and including any characteris-
25 tics identified by the voluntary risk manage-

1 ment framework for trustworthy artificial intel-
2 ligence systems, or successor framework, au-
3 thorized under subsection (c). Such practices
4 and norms may relate to the following:

5 “(i) Documentation of training and
6 evaluation datasets, such as information
7 and statistics about a dataset’s size,
8 curation, annotation, and sources, and the
9 protocols for a dataset’s selection, creators,
10 provenance, processing, augmentation, fil-
11 ters, inclusion of personally identifiable in-
12 formation, and intellectual property usage.

13 “(ii) Documentation of model infor-
14 mation, such as a model’s development
15 stages, training objectives, training strate-
16 gies, inference objectives, capabilities, re-
17 producibility of capabilities, input and out-
18 put modalities, components, size, and ar-
19 chitecture.

20 “(iii) Evaluation of benchmarks for
21 multi-metric assessments, such as an as-
22 sessment of an appropriate combination of
23 robustness, resilience, security, safety, fair-
24 ness, privacy, accuracy, validity, reliability,
25 accountability, usability, transparency, effi-

1 ciency, and calibration, and any character-
2 istics identified by the voluntary risk man-
3 agement framework for trustworthy artifi-
4 cial intelligence systems, or successor
5 framework, authorized under subsection
6 (c).

7 “(iv) Metrics and methodologies for
8 evaluations of artificial intelligence sys-
9 tems, such as establishing evaluation
10 datasets.

11 “(v) Public reporting of artificial in-
12 telligence systems’ capabilities, limitations,
13 and possible areas of appropriate and inap-
14 propriate use.

15 “(vi) Disclosure of security practices,
16 such as artificial intelligence red teaming
17 and third-party assessments, that were
18 used in the development of an artificial in-
19 telligence system.

20 “(vii) How to release to the public
21 components of an artificial intelligence sys-
22 tem or information about an artificial in-
23 telligence system, including aspects of the
24 model, associated training data, and li-
25 cense agreements.

1 “(viii) Approaches and channels for
2 collaboration and knowledge-sharing of
3 best practices across industry, govern-
4 ments, civil society, and academia.

5 “(ix) Such other categories as the Di-
6 rector determines appropriate and con-
7 sistent with this subsection.

8 “(C) For each practice and norm cat-
9 egorized and listed in accordance with subpara-
10 graph (B), provide recommendations and prac-
11 tices for utilizing such practice or norm.

12 “(2) IMPLEMENTATION.—In conducting the Di-
13 rector’s duties under paragraph (1), the Director
14 shall carry out the following:

15 “(A) Update the voluntary risk manage-
16 ment framework for trustworthy artificial intel-
17 ligence systems, or successor framework, au-
18 thorized under subsection (c) as the Director
19 determines appropriate.

20 “(B) Ensure that voluntary guidance de-
21 veloped in paragraph (1) is based on inter-
22 national standards and industry best practices
23 to the extent possible and practical.

1 “(C) Not prescribe or otherwise require the
2 use of specific information or communications
3 technology products or services.

4 “(D) Collaborate with public, industry, and
5 academic entities as the Director determines
6 appropriate, including conducting periodic out-
7 reach to receive public input from public, indus-
8 try, and academic stakeholders.

9 “(3) REPORT.—In conducting the Director’s
10 duties under paragraph (1), the Director shall, not
11 later than 18 months after the date of the enact-
12 ment of this subsection, brief the Committee on
13 Science, Space, and Technology of the House of
14 Representatives and the Committee on Commerce,
15 Science, and Transportation of the Senate on the
16 following:

17 “(A) New or updated materials, programs,
18 or systems that were produced as a result of
19 carrying out this subsection.

20 “(B) Policy recommendations of the Direc-
21 tor that could facilitate and improve commu-
22 nication and coordination between the private
23 sector and relevant Federal agencies regarding
24 implementing the recommended practices iden-
25 tified in this subsection.

1 “(4) DEFINITIONS.—In this subsection:

2 “(A) ARTIFICIAL INTELLIGENCE RED
3 TEAMING.—The term ‘artificial intelligence red
4 teaming’ means a structured testing of adver-
5 sarial efforts to find flaws and vulnerabilities in
6 an artificial intelligence system and identify
7 risks, flaws, and vulnerabilities of artificial in-
8 telligence systems, such as harmful outputs
9 from such system, unforeseen or undesirable
10 system behaviors, limitations, and potential
11 risks associated with the misuse of such system.

12 “(B) ARTIFICIAL INTELLIGENCE SYS-
13 TEM.—The term ‘artificial intelligence system’
14 has the meaning given such term in section
15 7223 of the Advancing American AI Act (40
16 U.S.C. 11301 note; as enacted as part of title
17 LXXII of division G of the James M. Inhofe
18 National Defense Authorization Act for Fiscal
19 Year 2023; Public Law 117–263).”.

○