

118TH CONGRESS
2D SESSION

H. R. 7394

To prohibit the use of trade secrets privileges to prevent defense access to evidence in criminal proceedings, provide for the establishment of Computational Forensic Algorithm Testing Standards and a Computational Forensic Algorithm Testing Program, and for other purposes.

IN THE HOUSE OF REPRESENTATIVES

FEBRUARY 15, 2024

Mr. TAKANO (for himself and Mr. EVANS) introduced the following bill; which was referred to the Committee on the Judiciary, and in addition to the Committee on Science, Space, and Technology, for a period to be subsequently determined by the Speaker, in each case for consideration of such provisions as fall within the jurisdiction of the committee concerned

A BILL

To prohibit the use of trade secrets privileges to prevent defense access to evidence in criminal proceedings, provide for the establishment of Computational Forensic Algorithm Testing Standards and a Computational Forensic Algorithm Testing Program, 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 “Justice in Forensic
5 Algorithms Act of 2024”.

1 **SEC. 2. COMPUTATIONAL FORENSIC ALGORITHM TESTING**
2 **STANDARDS.**

3 (a) IN GENERAL.—Not later than 1 year after the
4 date of enactment of this Act, the Director of the National
5 Institute of Standards and Technology shall establish a
6 program to provide for creation and maintenance of stand-
7 ards for testing computational forensic software, to be
8 known as the Computational Forensic Algorithm Testing
9 Standards, consistent with the following:

10 (1) Testing standards shall include an assess-
11 ment for the potential for disparate impact, on the
12 basis of race, ethnicity, socioeconomic status, gender,
13 and other demographic features.

14 (2) Testing standards shall address—

15 (A) the underlying scientific principles and
16 methods implemented in computational forensic
17 software; and

18 (B) requirements for testing the software
19 including the conditions under which it needs to
20 be tested, types of testing data to be used, test-
21 ing environments, testing methodologies, and
22 system performance statistics required to be re-
23 ported including—

24 (i) accuracy, including false positive
25 and false negative error rates;

26 (ii) precision;

1 (iii) reproducibility;

2 (iv) robustness;

3 (v) sensitivity; and

4 (vi) system failure rates;

5 (C) requirements for publicly available doc-
6 umentation by developers of computational fo-
7 rensic software of the purpose and function of
8 the software, the development process, including
9 source and description of data used to develop
10 the tool, and internal testing methodology and
11 results, including source and description of test-
12 ing data;

13 (D) requirements for laboratories and any
14 other entities using computational forensic soft-
15 ware to validate it for use, including to specify
16 the conditions under which the lab has vali-
17 dated it for their use, requirements for what in-
18 formation needs to be included in a public re-
19 port on the lab or other entity's validation, and
20 requirements for internal validation updates
21 when there are material changes to the soft-
22 ware; and

23 (E) requirements for reports provided to
24 defendants by prosecution produced docu-

1 menting the use and results of computational
2 forensic software used in individual cases.

3 (3) Testing standards shall be issued as a rule-
4 making under section 553 of title 5, United States
5 Code.

6 (4) The Director shall consult with outside ex-
7 perts in forensic science, bioethics, algorithmic dis-
8 crimination, data privacy, racial justice, criminal jus-
9 tice reform, exonerations, and other relevant areas
10 of expertise identified through public input.

11 (b) PROTECTION OF TRADE SECRETS.—

12 (1) There shall be no trade secret evidentiary
13 privilege to withhold relevant evidence in criminal
14 proceedings in the United States courts.

15 (2) Nothing in this section may be construed to
16 alter the standard operation of the Federal Rules of
17 Criminal Procedure, or the Federal Rules of Evi-
18 dence, as such rules would function in the absence
19 of an evidentiary privilege.

20 (c) REQUIREMENTS FOR FEDERAL USE OF FOREN-
21 SIC ALGORITHMS.—Any Federal law enforcement agency
22 or crime laboratory providing services to a Federal law
23 enforcement agency using computational forensic software
24 may use only software that has been tested under the Na-
25 tional Institute of Standards and Technology's Computa-

1 tional Forensic Algorithm Testing Program and shall con-
2 duct an internal validation according to the requirements
3 outlined in the Computational Forensic Algorithm Testing
4 Standards and make the results publicly available. The in-
5 ternal validation shall be updated when there is a material
6 change in the software that triggers a retesting by the
7 Computational Forensic Algorithm Testing Program.

8 (d) TESTING PROGRAM.—The Director of the Na-
9 tional Institute of Standards and Technology shall estab-
10 lish a Computational Forensic Algorithm Testing Pro-
11 gram, whose activities include the following:

12 (1) Testing individual software programs using
13 the testing requirements established in the Computa-
14 tional Forensic Algorithm Testing Standards.

15 (2) Using realistic sample testing data similar
16 to what would be used by law enforcement in crimi-
17 nal investigations in performing such testing, includ-
18 ing incomplete and contaminated samples.

19 (3) Using testing data that represents diversity
20 of racial, ethnic, and gender identities and intersec-
21 tions of these identities in performing such testing.

22 (4) Using testing data that tests the limits of
23 the software and demonstrates the boundaries of re-
24 liability described in the performance measures de-

1 fined in the Computational Forensic Algorithm Test-
2 ing Standards in performing such testing.

3 (5) Publishing the results of testing the soft-
4 ware online including results under conditions speci-
5 fied in the testing standards and across diversity of
6 racial, ethnic, and gender identities and intersections
7 of these identities in a publicly available format.

8 (e) TESTING FREQUENCY.—Retesting shall be con-
9 ducted when a material change is made to the software
10 that impacts its performance and may affect its outputs.
11 The Director shall establish requirements for determining
12 whether changes are material or nonmaterial.

13 (f) USE OF COMPUTATIONAL FORENSIC SOFT-
14 WARE.—Any results or reports resulting from analysis by
15 computational forensic software shall be provided to the
16 defendant, and the defendant shall be accorded access to
17 both an executable copy of and the source code for the
18 version of the computational forensic software—as well as
19 earlier versions of the software, necessary instructions for
20 use and interpretation of the results, and relevant files and
21 data—used for analysis in the case and suitable for testing
22 purposes. Such a report on the results shall include—

23 (1) the name of the company that developed the
24 software;

25 (2) the name of the lab where test was run;

1 (3) the version of the software that was used;

2 (4) the dates of the most recent changes to the
3 software and record of changes made, including any
4 bugs found in the software and what was done to
5 address those bugs;

6 (5) documentation of procedures followed based
7 on procedures outlined in internal validation;

8 (6) documentation of conditions under which
9 software was used relative to the conditions under
10 which software was tested; and

11 (7) any other information specified by the Di-
12 rector of the National Institute of Standards and
13 Technology in the Computational Forensic Algo-
14 rithm Testing Standards.

15 (g) INADMISSIBILITY OF CERTAIN EVIDENCE.—In
16 any criminal case, evidence that is the result of analysis
17 by computational forensic software is admissible only if—

18 (1) the computational forensic software used
19 has been submitted to the Computational Forensic
20 Algorithm Testing Program of the Director of the
21 National Institute of Standards and Technology and
22 there have been no material changes to that software
23 since it was last tested; and

24 (2) the developers and users of the computa-
25 tional forensic software agree to waive any and all

1 legal claims against the defense or any member of
2 its team for the purposes of the defense analyzing or
3 testing the computational forensic software.

4 (h) DEFINITIONS.—In this Act:

5 (1) COMPUTATIONAL FORENSIC SOFTWARE.—

6 The term “computational forensic software” means
7 software that relies on an automated or semiauto-
8 mated computational process, including one derived
9 from machine learning, statistics, or other data proc-
10 essing or artificial intelligence techniques, to process,
11 analyze, or interpret evidence.

12 (2) MATERIAL CHANGE.—The term “material
13 change” means an update to computational forensic
14 software that may affect the performance measures
15 defined in the Computational Forensic Algorithm
16 Testing Standards or the use or output of the soft-
17 ware.

18 (3) NONMATERIAL CHANGE.—The term “non-
19 material change” means an update to computational
20 forensic software that does not affect the perform-
21 ance measures, use, or output of the software.

○