

117TH CONGRESS
1ST SESSION

S. _____

To establish the National Deepfake and Digital Provenance Task Force,
and for other purposes.

IN THE SENATE OF THE UNITED STATES

_____ introduced the following bill; which was read twice
and referred to the Committee on _____

A BILL

To establish the National Deepfake and Digital Provenance
Task Force, 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 “Deepfake Task Force
5 Act”.

6 **SEC. 2. NATIONAL DEEFAKE AND DIGITAL PROVENANCE**
7 **TASK FORCE.**

8 (a) DEFINITIONS.—In this section:

9 (1) DIGITAL CONTENT FORGERY.—The term
10 “digital content forgery” means the use of emerging

1 technologies, including artificial intelligence and ma-
2 chine learning techniques, to fabricate or manipulate
3 audio, visual, or text content with the intent to mis-
4 lead.

5 (2) DIGITAL CONTENT PROVENANCE.—The
6 term “digital content provenance” means the
7 verifiable chronology of the origin and history of a
8 piece of digital content, such as an image, video,
9 audio recording, or electronic document.

10 (3) ELIGIBLE ENTITY.—The term “eligible enti-
11 ty” means—

12 (A) a private sector or nonprofit organiza-
13 tion; or

14 (B) an institution of higher education.

15 (4) INSTITUTION OF HIGHER EDUCATION.—The
16 term “institution of higher education” has the
17 meaning given the term in section 101 of the Higher
18 Education Act of 1965 (20 U.S.C. 1001).

19 (5) RELEVANT CONGRESSIONAL COMMIT-
20 TEES.—The term “relevant congressional commit-
21 tees” means—

22 (A) the Committee on Homeland Security
23 and Governmental Affairs of the Senate; and

1 (B) the Committee on Homeland Security
2 and the Committee on Oversight and Reform of
3 the House of Representatives.

4 (6) SECRETARY.—The term “Secretary” means
5 the Secretary of Homeland Security.

6 (7) TASK FORCE.—The term “Task Force”
7 means the National Deepfake and Provenance Task
8 Force established under subsection (b)(1).

9 (b) ESTABLISHMENT OF TASK FORCE.—

10 (1) ESTABLISHMENT.—The Secretary, in co-
11 ordination with the Director of the Office of Science
12 and Technology Policy, shall establish a task force,
13 to be known as “the National Deepfake Provenance
14 Task Force”, to—

15 (A) investigate the feasibility of, and obsta-
16 cles to, developing and deploying standards and
17 technologies for determining digital content
18 provenance;

19 (B) propose policy changes to reduce the
20 proliferation and impact of digital content for-
21 geries, such as the adoption of digital content
22 provenance and technology standards; and

23 (C) serve as a formal mechanism for inter-
24 agency coordination and information sharing to
25 facilitate the creation and implementation of a

1 national strategy to address the growing threats
2 posed by digital content forgeries.

3 (2) MEMBERSHIP.—

4 (A) CO-CHAIRPERSONS.—The following
5 shall serve as co-chairpersons of the Task
6 Force:

7 (i) The Secretary or a designee of the
8 Secretary.

9 (ii) The Director of the Office of
10 Science and Technology Policy or a des-
11 ignee of the Director.

12 (B) COMPOSITION.—The Task Force shall
13 be composed of 12 members, of whom—

14 (i) 4 shall be representatives from the
15 Federal Government, including the co-
16 chairpersons of the Task Force;

17 (ii) 4 shall be representatives from in-
18 stitutions of higher education; and

19 (iii) 4 shall be representatives from
20 private or nonprofit organizations.

21 (C) APPOINTMENT.—Not later than 120
22 days after the date of enactment of this Act,
23 the co-chairpersons of the Task Force shall ap-
24 point members to the Task Force in accordance

1 with subparagraph (A) from among technical
2 experts in—

3 (i) artificial intelligence;

4 (ii) media manipulation;

5 (iii) digital forensics;

6 (iv) secure digital content and deliv-
7 ery;

8 (v) cryptography; or

9 (vi) related subjects.

10 (D) TERM OF APPOINTMENT.—The term
11 of a member of the Task Force shall end on the
12 date described in subsection (g)(1).

13 (E) VACANCY.—Any vacancy occurring in
14 the membership of the Task Force shall be
15 filled in the same manner in which the original
16 appointment was made.

17 (F) EXPENSES FOR NON-FEDERAL MEM-
18 BERS.—Members of the Task Force described
19 in clauses (ii) and (iii) of subparagraph (B)
20 shall be allowed travel expenses, including per
21 diem in lieu of subsistence, at rates authorized
22 for employees under subchapter I of chapter 57
23 of title 5, United States Code, while away from
24 their homes or regular places of business in the
25 performance of services for the Task Force.

1 (c) COORDINATED PLAN.—

2 (1) IN GENERAL.—The Task Force shall de-
3 velop a coordinated plan to—

4 (A) reduce the proliferation and impact of
5 digital content forgeries, including by exploring
6 how the adoption of a digital content prove-
7 nance standard could assist with reducing the
8 proliferation of digital content forgeries;

9 (B) develop mechanisms for content cre-
10 ators to—

11 (i) cryptographically certify the au-
12 thenticity of original media and non-decep-
13 tive manipulations; and

14 (ii) enable the public to validate the
15 authenticity of original media and non-de-
16 ceptive manipulations to establish digital
17 content provenance; and

18 (C) increase the ability of internet compa-
19 nies, journalists, watchdog organizations, other
20 relevant entities, and members of the public
21 to—

22 (i) meaningfully scrutinize and iden-
23 tify potential digital content forgeries; and

1 (ii) relay trust and information about
2 digital content provenance to content con-
3 sumers.

4 (2) CONTENTS.—The plan required under para-
5 graph (1) shall include the following:

6 (A) A Government-wide research and de-
7 velopment agenda to—

8 (i) improve technologies and systems
9 to detect digital content forgeries; and

10 (ii) relay information about digital
11 content provenance to content consumers.

12 (B) An assessment of the feasibility of,
13 and obstacles to, the deployment of technologies
14 and systems to capture, preserve, and display
15 digital content provenance.

16 (C) An assessment of the feasibility of, and
17 challenges in, distinguishing between—

18 (i) benign or helpful alterations to
19 digital content; and

20 (ii) intentionally deceptive or obfus-
21 cating alterations to digital content.

22 (D) A discussion of best practices, includ-
23 ing any necessary standards, for the adoption
24 and effective use of technologies and systems to

1 determine digital content provenance and detect
2 digital content forgeries.

3 (E) Conceptual proposals for necessary re-
4 search projects and experiments to further de-
5 velop successful technology to ascertain digital
6 content provenance.

7 (F) Proposed policy changes, including
8 changes in law, to—

9 (i) incentivize the adoption of tech-
10 nologies, systems, open standards, or other
11 means to detect digital content forgeries
12 and determine digital content provenance;
13 and

14 (ii) reduce the incidence, proliferation,
15 and impact of digital content forgeries.

16 (G) Recommendations for models for pub-
17 lic-private partnerships to fight disinformation
18 and reduce digital content forgeries, including
19 partnerships that support and collaborate on—

20 (i) industry practices and standards
21 for determining digital content provenance;

22 (ii) digital literacy education cam-
23 paigns and user-friendly detection tools for
24 the public to reduce the proliferation and

1 impact of disinformation and digital con-
2 tent forgeries;

3 (iii) industry practices and standards
4 for documenting relevant research and
5 progress in machine learning; and

6 (iv) the means and methods for identi-
7 fying and addressing the technical and fi-
8 nancial infrastructure that supports the
9 proliferation of digital content forgeries,
10 such as inauthentic social media accounts
11 and bank accounts.

12 (H) An assessment of privacy and civil lib-
13 erties requirements associated with efforts to
14 deploy technologies and systems to determine
15 digital content provenance or reduce the pro-
16 liferation of digital content forgeries, including
17 statutory or other proposed policy changes.

18 (I) A determination of metrics to define
19 the success of—

20 (i) technologies or systems to detect
21 digital content forgeries;

22 (ii) technologies or systems to deter-
23 mine digital content provenance; and

1 (iii) other efforts to reduce the inci-
2 dence, proliferation, and impact of digital
3 content forgeries.

4 (d) CONSULTATIONS.—In carrying out subsection (c),
5 the Task Force shall consult with the following:

6 (1) The Director of the National Science Foun-
7 dation.

8 (2) The National Academies of Sciences, Engi-
9 neering, and Medicine.

10 (3) The Director of the National Institute of
11 Standards and Technology.

12 (4) The Director of the Defense Advanced Re-
13 search Projects Agency.

14 (5) The Director of the Intelligence Advanced
15 Research Projects Activity of the Office of the Direc-
16 tor of National Intelligence.

17 (6) The Secretary of Energy.

18 (7) The Secretary of Defense.

19 (8) The Attorney General.

20 (9) The Secretary of State.

21 (10) The Federal Trade Commission.

22 (11) The United States Trade Representative.

23 (12) Representatives from private industry and
24 nonprofit organizations.

1 (13) Representatives from institutions of higher
2 education.

3 (14) Such other individuals as the Task Force
4 considers appropriate.

5 (e) STAFF.—

6 (1) IN GENERAL.—Staff of the Task Force
7 shall be comprised of detailees with expertise in arti-
8 ficial intelligence or related fields from—

9 (A) the Department of Homeland Security;

10 (B) the Office of Science and Technology
11 Policy;

12 (C) the National Institute of Standards
13 and Technology; or

14 (D) any other Federal agency the co-chair-
15 persons of the Task Force consider appropriate
16 with the consent of the head of the Federal
17 agency.

18 (2) OTHER ASSISTANCE.—

19 (A) IN GENERAL.—The co-chairpersons of
20 the Task Force may enter into an agreement
21 with an eligible entity for the temporary assign-
22 ment of employees of the eligible entity to the
23 Task Force in accordance with this paragraph.

1 (B) APPLICATION OF ETHICS RULES.—An
2 employee of an eligible entity assigned to the
3 Task Force under subparagraph (A)—

4 (i) shall be considered a special Gov-
5 ernment employee for the purpose of Fed-
6 eral law, including—

7 (I) chapter 11 of title 18, United
8 States Code; and

9 (II) the Ethics in Government
10 Act of 1978 (5 U.S.C. App.); and

11 (ii) notwithstanding section 202(a) of
12 title 18, United States Code, may be as-
13 signed to the Task Force for a period of
14 not more than 2 years.

15 (C) FINANCIAL LIABILITY.—An agreement
16 entered into with an eligible entity under sub-
17 subparagraph (A) shall require the eligible entity to
18 be responsible for any costs associated with the
19 assignment of an employee to the Task Force.

20 (D) TERMINATION.—The co-chairpersons
21 of the Task Force may terminate the assign-
22 ment of an employee to the Task Force under
23 subparagraph (A) at any time and for any rea-
24 son.

25 (f) TASK FORCE REPORTS.—

1 (1) INTERIM REPORT.—

2 (A) IN GENERAL.—Not later than 1 year
3 after the date on which all of the appointments
4 have been made under subsection (b)(2)(C), the
5 Task Force shall submit to the President and
6 the relevant congressional committees an in-
7 terim report containing the findings, conclu-
8 sions, and recommendations of the Task Force.

9 (B) CONTENTS.—The report required
10 under subparagraph (A) shall include specific
11 recommendations for ways to reduce the pro-
12 liferation and impact of digital content for-
13 geries, including the deployment of technologies
14 and systems to determine digital content prove-
15 nance.

16 (2) FINAL REPORT.—Not later than 180 days
17 after the date of the submission of the interim re-
18 port under paragraph (1)(A), the Task Force shall
19 submit to the President and the relevant congress-
20 sional committees a final report containing the find-
21 ings, conclusions, and recommendations of the Task
22 Force, including the plan developed under subsection
23 (c).

24 (3) REQUIREMENTS.—With respect to each re-
25 port submitted under this subsection—

1 (A) the Task Force shall make the report
2 publicly available; and

3 (B) the report—

4 (i) shall be produced in an unclassi-
5 fied form; and

6 (ii) may include a classified annex.

7 (g) TERMINATION.—

8 (1) IN GENERAL.—The Task Force shall termi-
9 nate on the date that is 90 days after the date on
10 which the Task Force submits the final report under
11 subsection (f)(2).

12 (2) RECORDS.—Upon the termination of the
13 Task Force under paragraph (1), each record of the
14 Task Force shall become a record of the National
15 Archives and Records Administration.