

1 Title: To establish the National Deepfake and Digital Provenance Task Force, and for other
2 purposes.
3
4

5 Be it enacted by the Senate and House of Representatives of the United States of America in
6 Congress assembled,

7 SECTION 1. SHORT TITLE.

8 This Act may be cited as the “Deepfake Task Force Act”.

9 SEC. 2. NATIONAL DEEPPFAKE AND DIGITAL 10 PROVENANCE TASK FORCE.

11 (a) Definitions.—In this section:

12 (1) DIGITAL CONTENT FORGERY.—The term “digital content forgery” means the use of
13 emerging technologies, including artificial intelligence and machine learning techniques, to
14 fabricate or manipulate audio, visual, or text content with the intent to mislead.

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

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

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

22 (5) TASK FORCE.—The term “Task Force” means the National Deepfake and Provenance
23 Task Force established under subsection (b)(1).

24 (6) RELEVANT CONGRESSIONAL COMMITTEES.—The term “relevant Congressional
25 Committees” means the Homeland Security and Governmental Affairs Committee of the
26 Senate and the Committee on Homeland Security and the Committee on Oversight and
27 Reform of the House of Representatives.

28 (b) Establishment of Task Force.—

29 (1) ESTABLISHMENT.—The Secretary, in coordination with the Director of the Office of
30 Science and Technology Policy, shall establish a task force, to be known as “the National
31 Deepfake Provenance Task Force”, to—

32 (A) investigate the feasibility of, and obstacles to, developing and deploying
33 standards and technologies for verifying digital content provenance;

34 (B) propose policy changes to reduce the prevalence, and impact, of digital content
35 forgeries, such as the adoption of digital content provenance and technology standards;
36 and

37 (C) serve as a formal mechanism for interagency coordination and information
38 sharing to facilitate the creation and implementation of a national strategy to address

1 the growing threats posed by digital content forgeries.

2 (2) MEMBERSHIP.—

3 (A) CO-CHAIRPERSONS.—The Secretary, or the Secretary’s designee, and the
4 Director of the Office of Science and Technology Policy, or the Director’s designee,
5 shall serve as the co-chairpersons of the Task Force.

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

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

9 (ii) 4 shall be representatives from institutions of higher education; and

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

11 (C) APPOINTMENT.—Not later than 120 days after the date of enactment of this Act,
12 the co-chairpersons of the Task Force shall appoint members to the Task Force in
13 accordance with subparagraph (A) from among technical experts in—

14 (i) artificial intelligence;

15 (ii) media manipulation;

16 (iii) digital forensics;

17 (iv) secure digital content and delivery;

18 (v) cryptography; or

19 (vi) related subjects.

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

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

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

29 (c) Coordinated Plan.—

30 (1) IN GENERAL.—The Task Force shall develop a coordinated plan to—

31 (A) reduce the proliferation, and impact, of digital content forgeries, including by
32 exploring how the adoption of a digital content provenance standard could assist with
33 reducing the proliferation of digital content forgeries;

34 (B) develop mechanisms for content creators to—

35 (i) cryptographically certify the authenticity of original media and non-
36 deceptive manipulations; and

37 (ii) enable the public to validate the authenticity of original media and non-

- 1 deceptive manipulations to establish digital content provenance; and
- 2 (C) increase the ability of internet companies, journalists, watchdog organizations,
3 and other relevant entities, and members of the public, to meaningfully scrutinize and
4 identify potential digital content forgeries, and relay trust and information about digital
5 content provenance to content consumers.
- 6 (2) CONTENTS.—The plan required under paragraph (1) shall include the following:
- 7 (A) A Government-wide research and development agenda to—
- 8 (i) improve technologies to identify digital content forgeries; and
- 9 (ii) relay information about digital content provenance to content consumers.
- 10 (B) An assessment of the feasibility of, and obstacles to, the deployment of
11 technology to capture, preserve, and display digital content provenance.
- 12 (C) An assessment of the feasibility of, and challenges in, distinguishing between—
- 13 (i) benign or helpful alterations to digital content; and
- 14 (ii) intentionally deceptive or obfuscating alterations to digital content.
- 15 (D) A discussion of best practices, including any necessary standards, for the
16 adoption and effective use of technology to ascertain digital content provenance.
- 17 (E) Conceptual proposals for necessary research projects and experiments to further
18 develop successful technology to ascertain digital content provenance.
- 19 (F) Proposed policy changes, including changes in law, to—
- 20 (i) incentivize the adoption of technology, open standards, or other means to
21 detect digital content forgeries and determine digital content provenance; and
- 22 (ii) reduce the incidence and proliferation of digital content forgeries.
- 23 (G) Recommendations of of models for public-private partnerships to fight
24 disinformation and reduce digital content forgeries, including partnerships that support
25 and collaborate on—
- 26 (i) industry practices and standards for verifying the authenticity digital content
27 provenance;
- 28 (ii) digital literacy education campaigns and publicly available detection tools
29 to reduce the proliferation, and impact, of disinformation and digital content
30 forgeries;
- 31 (iii) industry practices and standards for documenting relevant research and
32 progress in machine learning; and
- 33 (iv) the means and methods for identifying and addressing the technical and
34 financial infrastructure that support the proliferation of digital content forgeries,
35 such as inauthentic social media accounts and bank accounts.
- 36 (H) An assessment of privacy and civil liberties requirements associated with efforts
37 to deploy technology to ascertain digital content provenance or reduce the proliferation
38 of digital content forgeries, including statutory or other proposed policy changes.

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

2 (i) technology to detect digital content forgeries;

3 (ii) technology to ascertain digital content provenance; and

4 (iii) other efforts to reduce the incidence, proliferation, and impact of digital
5 content forgeries.

6 (d) Consultations.—In carrying out subsection (c), the Task Force shall consult with the
7 following:

8 (1) The Director of the National Science Foundation.

9 (2) The National Academies of Sciences, Engineering, and Medicine.

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

11 (4) The Director of the Defense Advanced Research Projects Agency.

12 (5) The Director of the Intelligence Advanced Research Projects Activity of the Office of
13 the Director of National Intelligence.

14 (6) The Secretary of Energy.

15 (7) The Secretary of Defense.

16 (8) The Attorney General.

17 (9) The Secretary of State.

18 (10) The Federal Trade Commission.

19 (11) The United States Trade Representative.

20 (12) representatives from private industry.

21 (13) representatives from institutions of higher education.

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

23 (e) Staff.—

24 (1) IN GENERAL.—Staff of the Task Force shall be comprised of detailees with expertise
25 in artificial intelligence or related fields from—

26 (A) the Department of Homeland Security;

27 (B) the Office of Science and Technology Policy;

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

29 (D) any other Federal agency the co-chairpersons of the Task Force consider
30 appropriate with the consent of the head of the Federal agency.

31 (2) OTHER ASSISTANCE.—

32 (A) IN GENERAL.—The co-chairpersons of the Task Force may, with the agreement of
33 a private sector, nonprofit, or educational organization, arrange for the temporary
34 assignment of employees of the organization to the Task Force in accordance with the
35 requirements of (e)(2).

1 (B) APPLICATION OF ETHICS RULES.—An employee of an organization assigned under
2 (2)—

3 (i) shall be considered a special government employee for purposes of federal
4 law, including chapter 11 of title 18, United States Code, and the Ethics in Government
5 Act); and

6 (ii) Notwithstanding section 202(a) of title 18, United States Code, may be
7 assigned to the Task Force for a period of not longer than 2 years.

8 (C) FINANCIAL LIABILITY.—Any agreement under this paragraph shall require the
9 organization concerned to be responsible for all costs associated with the assignment of
10 an employee under this paragraph.

11 (D) IN GENERAL.—An assignment under this paragraph may, at any time and for any
12 reason, be terminated by the Co-Chairs of the Task Force or the organization concerned,
13 and shall be for a total period of not more than 2 years.

14 (f) Task Force Reports.—

15 (1) INTERIM REPORT.—

16 (A) IN GENERAL.—Not later than 1 year after the date on which all of the
17 appointments have been made under subsection (b)(2)(C), the Task Force shall make
18 publicly available and submit to the President and the relevant Congressional
19 Committees an interim report containing the findings, conclusions, and
20 recommendations of the Task Force.

21 (B) CONTENTS.—The report required under subparagraph (A) shall include specific
22 recommendations for ways to reduce the proliferation, and impact, of digital content
23 forgeries, including the deployment of technology to ascertain digital content
24 provenance.

25 (C) FORM OF REPORT.—Each report required under subparagraph (A) shall be
26 produced in unclassified form, but may contain a classified annex.

27 (2) FINAL REPORT.—Not later than 180 days after the date of the submission of the
28 interim report under paragraph (1)(A), the Task Force shall make publicly available and
29 submit to the President and the relevant Congressional Committees a final report containing
30 the findings, conclusions, and recommendations of the Task Force, including the plan
31 developed under subsection (c).

32 (C) FORM OF REPORT.—Each report required under subparagraph (A) shall be
33 produced in unclassified form, but may contain a classified annex.

34 (g) Termination.—

35 (1) IN GENERAL.—The Task Force shall terminate on the date that is 90 days after the
36 date on which the Task Force submits the final report under subsection (f)(2).

37 (2) RECORDS.—Upon the termination of the Task Force under paragraph (1), each record
38 of the Task Force shall become a record of the National Archives and Records
39 Administration.