

116TH CONGRESS
1ST SESSION

H. R. 5209

To direct the Under Secretary for Science and Technology of the Department of Homeland Security to design and administer a voluntary online terrorist content moderation exercise program, and for other purposes.

IN THE HOUSE OF REPRESENTATIVES

NOVEMBER 21, 2019

Mr. ROSE of New York (for himself, Mr. THOMPSON of Mississippi, Ms. CLARKE of New York, Miss RICE of New York, Ms. UNDERWOOD, Mr. PAYNE, and Ms. SLOTKIN) introduced the following bill; which was referred to the Committee on Homeland Security

A BILL

To direct the Under Secretary for Science and Technology of the Department of Homeland Security to design and administer a voluntary online terrorist content moderation exercise 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 “Raising the Bar Act
5 of 2019”.

1 **SEC. 2. HOMELAND SECURITY VOLUNTARY ONLINE TER-**
2 **RORIST CONTENT MODERATION EXERCISE**
3 **PROGRAM.**

4 (a) ESTABLISHMENT OF EXERCISE PROGRAM.—The
5 Under Secretary for Science and Technology of the De-
6 partment of Homeland Security, in consultation with the
7 Under Secretary for Strategy, Policy, and Plans, the Offi-
8 cer for Civil Rights and Civil Liberties, and the Privacy
9 Officer of the Department of Homeland Security, shall de-
10 sign and administer a voluntary online terrorist content
11 moderation exercise program. Under such program, the
12 Under Secretary for Science and Technology shall—

13 (1) enter into an agreement with the lead insti-
14 tution designated under subsection (b), under which
15 the lead institution shall carry out not fewer than
16 three four-week voluntary online terrorist content
17 moderation exercises during each calendar year; and

18 (2) establish objective criteria for how the lead
19 institution should use information submitted by
20 trusted flaggers and participating technology compa-
21 nies during an exercise conducted under the pro-
22 gram to rate each participating technology company
23 on—

24 (A) the adherence of the participating
25 technology company to the written online ter-

1 rorist content moderation policies and proce-
2 dures of that company;

3 (B) the compliance of the participating
4 technology company with the requirement to
5 conduct assessments and provide notice of such
6 assessments under subsection (d)(2); and

7 (C) such other factors relating to a partici-
8 pating technology company's performance in
9 the exercise as the Under Secretary for Science
10 and Technology determines appropriate.

11 (b) LEAD INSTITUTION.—

12 (1) IN GENERAL.—For purposes of the program
13 established under subsection (a), the Under Sec-
14 retary for Science and Technology, in consultation
15 with the Under Secretary for Strategy, Policy, and
16 Plans, shall seek to enter into an agreement with a
17 qualified institution that agrees to be designated as
18 the lead institution for purposes of the program.

19 (2) QUALIFIED INSTITUTION.—For purposes of
20 this section, an institution is qualified for designa-
21 tion as the lead institution pursuant to paragraph
22 (1) if such institution is an institution of higher edu-
23 cation or nonprofit institution that possesses dem-
24 onstrated expertise in at least two of the following
25 areas:

- 1 (A) Domestic terrorism.
- 2 (B) International terrorism.
- 3 (C) Cybersecurity.
- 4 (D) Computer or information technology.
- 5 (E) Privacy, civil rights, civil liberties, or
- 6 human rights.

7 (3) RESPONSIBILITIES.—Pursuant to an agree-
8 ment under this subsection, the lead institution shall
9 agree to carry out the following responsibilities:

10 (A) To identify and conduct outreach to
11 technology companies and potential trusted
12 flaggers to encourage the participation of such
13 companies and potential trusted flaggers in the
14 exercise program under this section.

15 (B) To establish criteria, in consultation
16 with participating technology companies, for
17 qualified trusted flaggers.

18 (C) To schedule and carry out three four-
19 week exercises during each calendar year to
20 evaluate the adherence of each participating
21 technology company to the written online ter-
22 rorist content moderation policies and proce-
23 dures of the company during the period for
24 which the exercise is conducted, which shall in-
25 clude notifying participating technology compa-

1 nies and trusted flaggers of the commencement
2 of the exercise 24 hours before the commence-
3 ment of the exercise and may include providing
4 nominal payments to trusted flaggers for par-
5 ticipating in such exercise.

6 (D) To develop a letter rating system
7 based on the objective criteria established pur-
8 suant to subsection (a)(2), in collaboration with
9 participating technology companies, to be used
10 to assign a letter rating to each participating
11 technology company upon the conclusion of an
12 exercise.

13 (E) To establish a process under which a
14 trusted flagger can anonymously notify a par-
15 ticipating technology company of content that
16 the trusted flagger identifies during an exercise
17 because the trusted flagger believes such con-
18 tent is online terrorist content that violates a
19 written online terrorist content moderation pol-
20 icy or procedure of the company.

21 (F) To design a template for trusted
22 flaggers to use to submit to the lead institution
23 each notification communicated pursuant to the
24 process under subparagraph (E) together with
25 the following information:

1 (i) The name of the trusted flagger
2 communicating the notification and the
3 name of the participating technology com-
4 pany receiving such notification.

5 (ii) The grounds for the notification,
6 including a specific identification of the
7 written online terrorist content moderation
8 policy or procedure of the participating
9 technology company that was violated by
10 the identified content and the terrorist ide-
11 ology or ideologies associated with such
12 content.

13 (iii) The location, including the uni-
14 form resource locator, where the identified
15 content was found, including a screen shot
16 of the content that does not include any
17 personally identifiable information.

18 (iv) The date and time when the par-
19 ticipating technology company was notified
20 of such content pursuant to the process
21 under subparagraph (E).

22 (v) Any other information the lead in-
23 stitution determines is appropriate.

1 (G) To establish requirements for an as-
2 sessment as required pursuant to subsection
3 (d)(2).

4 (H) To issue a report pursuant to sub-
5 section (f) on each exercise after sharing a
6 draft of the report and providing participating
7 technology companies and trusted flaggers who
8 participated in the exercise with the opportunity
9 to comment on the report.

10 (I) Not later than 60 days after issuing a
11 report pursuant to subsection (f) on an exer-
12 cise, to convene a virtual or in-person meeting
13 with participating technology companies and
14 trusted flaggers who participated in the exercise
15 to discuss the exercise and other related mat-
16 ters, as identified by the lead institution, in
17 consultation with the participating technology
18 companies and trusted flaggers.

19 (4) CONSORTIUM.—An agreement entered into
20 under subsection (a)(1) may provide that the lead
21 institution may execute agreements with other insti-
22 tutions of higher education or nonprofit institutions
23 to establish a consortium of such institutions to as-
24 sist in carrying out the responsibilities of the lead
25 institution under the agreement. To the extent that

1 the Under Secretary for Science and Technology
2 identifies institutions of higher education or non-
3 profit institutions for participation in such a consor-
4 tium, the Under Secretary shall seek to ensure the
5 participation of historically Black colleges and uni-
6 versities, Hispanic-serving institutions, and Tribally
7 controlled colleges and universities.

8 (c) TRUSTED FLAGGERS.—

9 (1) IN GENERAL.—For purposes of the program
10 under this section, a trusted flagger is an individual
11 or entity that—

12 (A) is selected by the lead institution, in
13 coordination with participating technology com-
14 panies, on the basis of criteria established by
15 the institution for such purpose; and

16 (B) enters into an agreement with the lead
17 institution and the participating technology
18 companies that participate in an exercise car-
19 ried out under the program to perform the re-
20 sponsibilities specified in paragraph (2) for the
21 duration of the exercise.

22 (2) RESPONSIBILITIES.—The responsibilities
23 specified in this paragraph are the following:

24 (A) To monitor public-facing areas of the
25 participating technology companies for online

1 terrorist content that may violate a written on-
2 line terrorist content moderation policy or pro-
3 cedure of the participating technology company.

4 (B) To provide timely notification of any
5 online terrorist content identified on the online
6 platform of a participating technology company
7 to such company pursuant to the process under
8 subsection (b)(3)(E).

9 (C) To carry out other activities requested
10 by the lead institution, in consultation with par-
11 ticipating technology companies.

12 (d) RESPONSIBILITIES OF PARTICIPATING TECH-
13 NOLOGY COMPANIES.—

14 (1) AGREEMENTS.—To participate in the vol-
15 untary online terrorist content moderation exercise
16 program under this section, a technology company
17 shall enter into an agreement with the lead institu-
18 tion to carry out the responsibilities under this sub-
19 section.

20 (2) ASSESSMENTS.—Each participating tech-
21 nology company shall agree—

22 (A) to conduct an assessment of each noti-
23 fication communicated by a trusted flagger pur-
24 suant to the process established under sub-

1 section (b)(3)(E) within 24 hours of receipt;
2 and

3 (B) to provide notice to the lead institution
4 of the completion of each assessment conducted
5 under this paragraph, including—

6 (i) whether such assessment was com-
7 pleted within 24 hours of receipt of the no-
8 tification; and

9 (ii) whether such assessment caused
10 the participating technology company to
11 decide to take or not take a certain action
12 and the grounds for such action or in ac-
13 tion.

14 (3) PROVISION OF INFORMATION TO LEAD IN-
15 STITUTION.—Each participating technology company
16 shall agree to provide to the lead institution—

17 (A) the written online terrorist content
18 moderation policies and procedures of the com-
19 pany with respect to responding to identified
20 online terrorist content, including any rule or
21 community standard of the company that pro-
22 hibits terrorist content and information regard-
23 ing any system that the company uses to review
24 online terrorist content that is reported that
25 violates any such rule or standard, including—

1 (i) guidance about what online ter-
2 rorist content is prohibited, including ex-
3 amples of permissible and impermissible
4 content and the guidelines used internally
5 to enforce rules or community standards
6 that prohibit online terrorist content; and

7 (ii) information on the use of auto-
8 mated detection on the platform of the
9 company; and

10 (B) a point of contact for use by trusted
11 flaggers to report online terrorist content pur-
12 suant to the process under subsection
13 (b)(3)(E).

14 (4) DISCLOSURE AND NOTICE REQUIRE-
15 MENTS.—

16 (A) DISCLOSURE OF PARTICIPATION.—

17 Each such participating technology company
18 shall agree to disclose the participation of the
19 company in the voluntary online terrorist con-
20 tent moderation exercise program on the online
21 platform of the company.

22 (B) NOTICE TO USERS.—Each such par-

23 ticipating technology company shall agree to
24 provide notice to each user whose content is re-
25 moved or account is suspended or terminated as

1 a result of an exercise conducted under this sec-
2 tion. Such notice shall include—

3 (i) the specific provision in the written
4 online terrorist content moderation policies
5 or procedures of the participating tech-
6 nology company that such online terrorist
7 content was found to violate; and

8 (ii) an explanation of the process
9 through which the user can appeal, pursu-
10 ant to paragraph (5), the decision to re-
11 move the content or suspend or terminate
12 the account.

13 (C) FORM OF NOTICE.—Each such partici-
14 pating technology company shall agree to pro-
15 vide the notice required under subparagraph
16 (B) in both human- and machine-readable for-
17 mats that are accessible even if a user’s account
18 is suspended or terminated.

19 (5) APPEALS PROCESS.—Each participating
20 technology company shall agree to provide for a
21 timely appeal process under which a user may chal-
22 lenge a content removal or account suspension or
23 termination. Such process shall include—

24 (A) the review of the decision to remove
25 content or suspend an account by a person or

1 panel of persons who was not involved in the
2 initial decision;

3 (B) the provision to the user of an oppor-
4 tunity to present additional information that
5 will be considered in the review; and

6 (C) the provision to the user of notice of
7 the decision made in the appeals process, in-
8 cluding a statement of the reasoning sufficient
9 to allow the user to understand the decision.

10 (e) TRANSPARENCY.—The Under Secretary for
11 Science and Technology shall ensure that agreements
12 under this section shall require that before engaging in
13 an exercise under this section, the lead institution, an in-
14 stitution participating in a consortium under subsection
15 (b)(4), and each trusted flagger agree to disclose to the
16 Under Secretary any fiduciary or business relationship be-
17 tween such institution or trusted flagger and any partici-
18 pating technology company during the two-year period
19 preceding the date of the exercise.

20 (f) REPORTS.—

21 (1) REPORT REQUIRED.—Not later than 60
22 days after the last day of any voluntary online ter-
23 rorist content moderation exercise conducted under
24 this section, the lead institution, in consultation with

1 the participating technology companies and trusted
2 flaggers, shall—

3 (A) produce a report on the voluntary on-
4 line terrorist content moderation exercise;

5 (B) publish such report on the public
6 website of the lead institution; and

7 (C) transmit a copy of such report to—

8 (i) the Under Secretary for Science
9 and Technology for publication on the pub-
10 lic website of the Department of Homeland
11 Security; and

12 (ii) the Comptroller General of the
13 United States.

14 (2) CONTENTS OF REPORT.—Each report under
15 paragraph (1) shall include each of the following
16 with respect to the exercise covered by the report:

17 (A) A rating based on the letter rating sys-
18 tem developed pursuant to subsection (b)(3)(D),
19 for each participating technology company that
20 participated in the exercise.

21 (B) Information about—

22 (i) the total number of notifications
23 communicated to each participating tech-
24 nology company during the exercise;

1 (ii) the number of notifications that
2 were assessed by each participating tech-
3 nology company within 24 hours of receipt
4 as violating or not violating an online ter-
5 rorist content moderation policy or proce-
6 dure of the company and the basis for each
7 notification, including the violation of the
8 written online terrorist content moderation
9 policies or procedures and ideology or
10 ideologies associated with the content, for
11 such assessment; and

12 (iii) the number of notifications that
13 were assessed after 24 hours of receipt as
14 violating or not violating an online terrorist
15 content moderation policy or procedure of
16 the company and the basis for each notifi-
17 cation, including the violation of the writ-
18 ten online terrorist content moderation
19 policies or procedures and ideology or
20 ideologies associated with the content, for
21 such assessment.

22 (C) Information about any online terrorist
23 content that a participating technology com-
24 pany removes from a platform of the company
25 for violating an online terrorist content modera-

tion policy or procedure of the company during
the exercise, including—

(i) the number of posts deleted and
accounts suspended or terminated by a
participating technology company for vio-
lating a written online terrorist content
moderation policy or procedure of the com-
pany, disaggregated by whether flagged by
a trusted flagger, internally within the
technology company by an employee, by a
contractor, by a law enforcement official,
by a user, or through automated detection;

(ii) the number of discrete posts and
accounts flagged, and the number of dis-
crete posts removed and accounts sus-
pended or terminated, by a participating
technology company for violating the writ-
ten online terrorist content moderation
policies or procedures of the company,
disaggregated by information on the spe-
cific violation identified in the written on-
line terrorist content moderation policies or
procedures and the terrorist ideology or
ideologies associated with the post or ac-
count, disaggregated by whether flagged by

1 a trusted flagger, internally within the par-
2 ticipating technology company by an em-
3 ployee or contractor, by a law enforcement
4 official, by a user, or through automated
5 detection;

6 (iii) the number of discrete posts and
7 accounts flagged, and number of discrete
8 posts removed and accounts suspended or
9 terminated by a participating technology
10 company for violating the written online
11 terrorist content moderation policies or
12 procedures of the company, disaggregated
13 by the format of the content, such as text,
14 audio, image, video, or live stream; and

15 (iv) in the case of each exercise after
16 the initial exercise, an evaluation of
17 changes over time with respect to each cat-
18 egory of information referred to in clauses
19 (i) through (iii).

20 (D) Information on the exercise, including
21 the dates of the exercise and names of the
22 trusted flaggers that participated, together with
23 information on how many notifications each
24 such trusted flagger submitted during the exer-
25 cise.

1 (E) The written online terrorist content
2 moderation policies and procedures of each of
3 the participating technology companies, to-
4 gether with the corresponding definition for on-
5 line terrorist content adopted by each of the
6 participating technology companies, and a de-
7 scription of the appeals process of each such
8 company as required pursuant to subsection
9 (d)(5).

10 (F) Any identifiable trends and analysis
11 developed from conducting the exercise, as de-
12 termined appropriate by the lead institution, in
13 consultation with participating technology com-
14 panies and trusted flaggers.

15 (G) Any information provided by a partici-
16 pating technology company regarding efforts of
17 the company to—

18 (i) counter terrorist narratives and en-
19 hance technological capabilities to identify
20 and counter online terrorism content;

21 (ii) maintain policies or procedures
22 within the company that—

23 (I) prioritize the mental health of
24 individuals working within the com-
25 pany who participate in the efforts to

1 implement the written online terrorist
2 content moderation policies or proce-
3 dures of the company; and

4 (II) make available voluntary
5 mental health support, as needed, to
6 such employees and to contractors
7 and trusted flaggers; and

8 (iii) any other information determined
9 appropriate by the lead institution.

10 (3) FORMAT.—Each report under this sub-
11 section shall be made available in both a human-
12 and a machine-readable format.

13 (4) BRIEFINGS.—Not later than 30 days after
14 receiving a report under paragraph (1)(C)(i), the
15 Under Secretary for Science and Technology, in con-
16 sultation with the Under Secretary for Strategy,
17 Policy, and Plans, shall provide to the Committee on
18 Homeland Security of the House of Representatives
19 and the Committee on Homeland Security and Gov-
20 ernmental Affairs of the Senate a briefing on the
21 voluntary online terrorist content moderation exer-
22 cise program under this section.

23 (g) PUBLIC-PRIVATE PARTNERSHIP.—

24 (1) IN GENERAL.—The Under Secretary for
25 Science and Technology is authorized to enter into—

1 (A) an agreement using other transactional
2 authority with the lead institution for purposes
3 of carrying out this section; and

4 (B) public-private partnerships with par-
5 ticipating technology companies in which par-
6 ticipating technology companies agree provide
7 at least 80 percent of the funding to carry out
8 this section.

9 (2) OTHER TRANSACTIONAL AUTHORITY.—In
10 this subsection, the term “other transactional au-
11 thority” means the authority under section 831 of
12 the Homeland Security Act of 2002 (6 U.S.C. 391).

13 (h) AUTHORIZATION OF APPROPRIATIONS.—There is
14 authorized to be appropriated to carry out this Act—

15 (1) \$300,000 for fiscal year 2020; and

16 (2) \$150,000 for each of fiscal years 2021
17 through 2026.

18 (i) RULE OF CONSTRUCTION.—Nothing in the Act
19 shall be construed as—

20 (1) requiring participating technology compa-
21 nies to adopt standards for the moderation of online
22 terrorist content;

23 (2) authorizing the Department of Homeland
24 Security to participate in decision making regarding

1 the removal of content by participating technology
2 companies;

3 (3) requiring participating technology compa-
4 nies to provide user content to the Department of
5 Homeland Security, any institution participating in
6 the exercise program, or any other Federal, State,
7 local, tribal, or territorial government or inter-
8 national body; or

9 (4) authorizing the Department of Homeland
10 Security to allow subjective judgments regarding the
11 treatment of online content by a participating tech-
12 nology company in the objective criteria established
13 pursuant to subsection (a)(2).

14 (j) DEFINITIONS.—In this section:

15 (1) The term “Hispanic-serving institution” has
16 the meaning given such term in section 502(a) of
17 the Higher Education Act of 1965 (20 U.S.C.
18 1101a(a)).

19 (2) The term “historically Black colleges and
20 universities” means a part B institution described in
21 section 322(2) of the Higher Education Act of 1965
22 (20 U.S.C. 1061(2)).

23 (3) The term “institution of higher education”
24 has the meaning given such term in section 101 of

1 the Higher Education Act of 1965 (20 U.S.C.
2 1001).

3 (4) The term “online terrorist content” shall be
4 defined by each technology company participating in
5 an exercise under this section with respect to a plat-
6 form of the company in the community guidelines,
7 terms of service, or relevant policy applicable to such
8 platform.

9 (5) The term “personally identifiable informa-
10 tion” means any information about an individual
11 elicited, collected, stored, or maintained by an agen-
12 cy or owner or operator of a participating technology
13 company, including the following:

14 (A) Any information that can be used to
15 distinguish or trace the identity of an indi-
16 vidual, such as a name, social security number,
17 date or place of birth, mother’s maiden name,
18 telephone number, or biometric records.

19 (B) Any other information that is linked or
20 linkable to an individual, such as medical, edu-
21 cational, financial, or employment information.

22 (6) The term “participating technology com-
23 pany” means a business entity that owns or operates
24 any public-facing website, web application, or digital
25 application, including a mobile application, social

1 network, advertising network, search engine, or
2 email service that participates in the voluntary on-
3 line terrorist content moderation exercise program
4 under this Act.

5 (7) The term “Tribally controlled college or
6 university” has the meaning given such term in sec-
7 tion 2 of the Tribally Controlled Colleges and Uni-
8 versities Assistance Act of 1978 (25 U.S.C. 1801).

9 (k) SUNSET.—The authority to carry out this section
10 shall terminate on the date that is seven years after the
11 date of the enactment of this Act.

12 **SEC. 3. COMPTROLLER GENERAL REPORT.**

13 Not later than 180 days after the Comptroller Gen-
14 eral of the United States receives the sixth report under
15 section 2(f), the Comptroller General shall submit to Con-
16 gress a report on the implementation of section 2.

○