I

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.

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

**SECTION 1. SHORT TITLE.**

This Act may be cited as the ''Raising the Bar Act of 2019''.

**SEC. 2. HOMELAND SECURITY VOLUNTARY ONLINE TERRORIST CONTENT MODERATION EXERCISE PROGRAM.**

(a) ESTABLISHMENT OF EXERCISE PROGRAM.—The Under Secretary for Science and Technology of the Department of Homeland Security, in consultation with the Under Secretary for Strategy, Policy, and Plans, the Officer for Civil Rights and Civil Liberties, and the Privacy Officer of the Department of Homeland Security, shall design and administer a voluntary online terrorist content moderation exercise program. Under such program, the Under Secretary for Science and Technology shall—

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

(2) establish objective criteria for how the lead institution should use information submitted by trusted flaggers and participating technology companies during an exercise conducted under the program to rate each participating technology company on—

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

rorist content moderation policies and procedures of that company;

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

(C) such other factors relating to a participating technology company's performance in the exercise as the Under Secretary for Science and Technology determines appropriate.

(b) LEAD INSTITUTION.—

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

(2) QUALIFIED INSTITUTION.—For purposes of this section, an institution is qualified for designation as the lead institution pursuant to paragraph (1) if such institution is an institution of higher education or nonprofit institution that possesses demonstrated expertise in at least two of the following areas:

(A) Domestic terrorism.

(B) International terrorism.

(C) Cybersecurity.

(D) Computer or information technology.

(E) Privacy, civil rights, civil liberties, or human rights.

(3) RESPONSIBILITIES.—Pursuant to an agreement under this subsection, the lead institution shall agree to carry out the following responsibilities:

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

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

(C) To schedule and carry out three four-week exercises during each calendar year to evaluate the adherence of each participating technology company to the written online terrorist content moderation policies and procedures of the company during the period for which the exercise is conducted, which shall include notifying participating technology compa-

nies and trusted flaggers of the commencement of the exercise 24 hours before the commencement of the exercise and may include providing nominal payments to trusted flaggers for participating in such exercise.

(D) To develop a letter rating system based on the objective criteria established pursuant to subsection (a)(2), in collaboration with participating technology companies, to be used to assign a letter rating to each participating technology company upon the conclusion of an exercise.

(E) To establish a process under which a trusted flagger can anonymously notify a participating technology company of content that the trusted flagger identifies during an exercise because the trusted flagger believes such content is online terrorist content that violates a written online terrorist content moderation policy or procedure of the company.

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

(i) The name of the trusted flagger communicating the notification and the name of the participating technology company receiving such notification.

(ii) The grounds for the notification, including a specific identification of the written online terrorist content moderation policy or procedure of the participating technology company that was violated by the identified content and the terrorist ideology or ideologies associated with such content.

(iii) The location, including the uniform resource locator, where the identified content was found, including a screen shot of the content that does not include any personally identifiable information.

(iv) The date and time when the participating technology company was notified of such content pursuant to the process under subparagraph (E).

(v) Any other information the lead institution determines is appropriate.

(G) To establish requirements for an assessment as required pursuant to subsection (d)(2).

(H) To issue a report pursuant to subsection (f) on each exercise after sharing a draft of the report and providing participating technology companies and trusted flaggers who participated in the exercise with the opportunity to comment on the report.

(I) Not later than 60 days after issuing a report pursuant to subsection (f) on an exercise, to convene a virtual or in-person meeting with participating technology companies and trusted flaggers who participated in the exercise to discuss the exercise and other related matters, as identified by the lead institution, in consultation with the participating technology companies and trusted flaggers.

(4) CONSORTIUM.—An agreement entered into under subsection (a)(1) may provide that the lead institution may execute agreements with other institutions of higher education or nonprofit institutions to establish a consortium of such institutions to assist in carrying out the responsibilities of the lead institution under the agreement. To the extent that

the Under Secretary for Science and Technology identifies institutions of higher education or nonprofit institutions for participation in such a consortium, the Under Secretary shall seek to ensure the participation of historically Black colleges and universities, Hispanic-serving institutions, and Tribally controlled colleges and universities.

(c) TRUSTED FLAGGERS.—

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

(A) is selected by the lead institution, in coordination with participating technology companies, on the basis of criteria established by the institution for such purpose; and

(B) enters into an agreement with the lead institution and the participating technology companies that participate in an exercise carried out under the program to perform the responsibilities specified in paragraph (2) for the duration of the exercise.

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

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

terrorist content that may violate a written online terrorist content moderation policy or procedure of the participating technology company.

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

(C) To carry out other activities requested by the lead institution, in consultation with participating technology companies.

(d) RESPONSIBILITIES OF PARTICIPATING TECHNOLOGY COMPANIES.—

(1) AGREEMENTS.—To participate in the voluntary online terrorist content moderation exercise program under this section, a technology company shall enter into an agreement with the lead institution to carry out the responsibilities under this subsection.

(2) ASSESSMENTS.—Each participating technology company shall agree—

(A) to conduct an assessment of each notification communicated by a trusted flagger pursuant to the process established under sub-

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

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

(i) whether such assessment was completed within 24 hours of receipt of the notification; and

(ii) whether such assessment caused the participating technology company to decide to take or not take a certain action and the grounds for such action or in action.

(3) PROVISION OF INFORMATION TO LEAD INSTITUTION.—Each participating technology company shall agree to provide to the lead institution—

(A) the written online terrorist content moderation policies and procedures of the company with respect to responding to identified online terrorist content, including any rule or community standard of the company that prohibits terrorist content and information regarding any system that the company uses to review online terrorist content that is reported that violates any such rule or standard, including—

(i) guidance about what online terrorist content is prohibited, including examples of permissible and impermissible content and the guidelines used internally to enforce rules or community standards that prohibit online terrorist content; and

(ii) information on the use of automated detection on the platform of the company; and

(B) a point of contact for use by trusted flaggers to report online terrorist content pursuant to the process under subsection (b)(3)(E).

(4) DISCLOSURE AND NOTICE REQUIREMENTS.—

(A) DISCLOSURE OF PARTICIPATION.—Each such participating technology company shall agree to disclose the participation of the company in the voluntary online terrorist content moderation exercise program on the online platform of the company.

(B) NOTICE TO USERS.—Each such participating technology company shall agree to provide notice to each user whose content is removed or account is suspended or terminated as

a result of an exercise conducted under this section. Such notice shall include—

(i) the specific provision in the written online terrorist content moderation policies or procedures of the participating technology company that such online terrorist content was found to violate; and

(ii) an explanation of the process through which the user can appeal, pursuant to paragraph (5), the decision to remove the content or suspend or terminate the account.

(C) FORM OF NOTICE.—Each such participating technology company shall agree to provide the notice required under subparagraph (B) in both human- and machine-readable formats that are accessible even if a user's account is suspended or terminated.

(5) APPEALS PROCESS.—Each participating technology company shall agree to provide for a timely appeal process under which a user may challenge a content removal or account suspension or termination. Such process shall include—

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

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

(B) the provision to the user of an opportunity to present additional information that will be considered in the review; and

(C) the provision to the user of notice of the decision made in the appeals process, including a statement of the reasoning sufficient to allow the user to understand the decision.

(e) TRANSPARENCY.—The Under Secretary for Science and Technology shall ensure that agreements under this section shall require that before engaging in an exercise under this section, the lead institution, an institution participating in a consortium under subsection (b)(4), and each trusted flagger agree to disclose to the Under Secretary any fiduciary or business relationship between such institution or trusted flagger and any participating technology company during the two-year period preceding the date of the exercise.

(f) REPORTS.—

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

the participating technology companies and trusted flaggers, shall—

(A) produce a report on the voluntary online terrorist content moderation exercise;

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

(C) transmit a copy of such report to—

(i) the Under Secretary for Science and Technology for publication on the public website of the Department of Homeland Security; and

(ii) the Comptroller General of the United States.

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

(A) A rating based on the letter rating system developed pursuant to subsection (b)(3)(D), for each participating technology company that participated in the exercise.

(B) Information about—

(i) the total number of notifications communicated to each participating technology company during the exercise;

(ii) the number of notifications that were assessed by each participating technology company within 24 hours of receipt as violating or not violating an online terrorist content moderation policy or procedure of the company and the basis for each notification, including the violation of the written online terrorist content moderation policies or procedures and ideology or ideologies associated with the content, for such assessment; and

(iii) the number of notifications that were assessed after 24 hours of receipt as violating or not violating an online terrorist content moderation policy or procedure of the company and the basis for each notification, including the violation of the written online terrorist content moderation policies or procedures and ideology or ideologies associated with the content, for such assessment.

(C) Information about any online terrorist content that a participating technology company removes from a platform of the company 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 violating a written online terrorist content moderation policy or procedure of the company, 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 discrete posts removed and accounts suspended or terminated, by a participating technology company for violating the written online terrorist content moderation policies or procedures of the company, disaggregated by information on the specific violation identified in the written online terrorist content moderation policies or procedures and the terrorist ideology or ideologies associated with the post or account, disaggregated by whether flagged by

a trusted flagger, internally within the participating technology company by an employee or contractor, by a law enforcement official, by a user, or through automated detection;

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

(iv) in the case of each exercise after the initial exercise, an evaluation of changes over time with respect to each category of information referred to in clauses (i) through (iii).

(D) Information on the exercise, including the dates of the exercise and names of the trusted flaggers that participated, together with information on how many notifications each such trusted flagger submitted during the exercise.

(E) The written online terrorist content moderation policies and procedures of each of the participating technology companies, together with the corresponding definition for online terrorist content adopted by each of the participating technology companies, and a description of the appeals process of each such company as required pursuant to subsection (d)(5).

(F) Any identifiable trends and analysis developed from conducting the exercise, as determined appropriate by the lead institution, in consultation with participating technology companies and trusted flaggers.

(G) Any information provided by a participating technology company regarding efforts of the company to—

(i) counter terrorist narratives and enhance technological capabilities to identify and counter online terrorism content;

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

(I) prioritize the mental health of individuals working within the company who participate in the efforts to

implement the written online terrorist content moderation policies or procedures of the company; and

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

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

(3) FORMAT.—Each report under this subsection shall be made available in both a human- and a machine-readable format.

(4) BRIEFINGS.—Not later than 30 days after receiving a report under paragraph (1)(C)(i), the Under Secretary for Science and Technology, in consultation with the Under Secretary for Strategy, Policy, and Plans, shall provide to the Committee on Homeland Security of the House of Representatives and the Committee on Homeland Security and Governmental Affairs of the Senate a briefing on the voluntary online terrorist content moderation exercise program under this section.

(g) PUBLIC-PRIVATE PARTNERSHIP.—

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

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

(B) public-private partnerships with participating technology companies in which participating technology companies agree provide at least 80 percent of the funding to carry out this section.

(2) OTHER TRANSACTIONAL AUTHORITY.—In this subsection, the term ''other transactional authority'' means the authority under section 831 of the Homeland Security Act of 2002 (6 U.S.C. 391).

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

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

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

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

(1) requiring participating technology companies to adopt standards for the moderation of online terrorist content;

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

the removal of content by participating technology companies;

(3) requiring participating technology companies to provide user content to the Department of Homeland Security, any institution participating in the exercise program, or any other Federal, State, local, tribal, or territorial government or international body; or

(4) authorizing the Department of Homeland Security to allow subjective judgments regarding the treatment of online content by a participating technology company in the objective criteria established pursuant to subsection (a)(2).

(j) DEFINITIONS.—In this section:

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

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

(3) The term ''institution of higher education'' has the meaning given such term in section 101 of

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

(4) The term ''online terrorist content'' shall be defined by each technology company participating in an exercise under this section with respect to a platform of the company in the community guidelines, terms of service, or relevant policy applicable to such platform.

(5) The term ''personally identifiable information'' means any information about an individual elicited, collected, stored, or maintained by an agency or owner or operator of a participating technology company, including the following:

(A) Any information that can be used to distinguish or trace the identity of an individual, such as a name, social security number, date or place of birth, mother's maiden name, telephone number, or biometric records.

(B) Any other information that is linked or linkable to an individual, such as medical, educational, financial, or employment information.

(6) The term ''participating technology company'' means a business entity that owns or operates any public-facing website, web application, or digital application, including a mobile application, social

network, advertising network, search engine, or email service that participates in the voluntary online terrorist content moderation exercise program under this Act.

(7) The term ''Tribally controlled college or university'' has the meaning given such term in section 2 of the Tribally Controlled Colleges and Universities Assistance Act of 1978 (25 U.S.C. 1801).

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

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

Not later than 180 days after the Comptroller General of the United States receives the sixth report under section 2(f), the Comptroller General shall submit to Congress a report on the implementation of section 2.

○