reason to the agency designated or established under subsection (b)(2).

(b) REPORTING PROCESS.—

(1) IN GENERAL.—The Attorney General shall establish a process by which a provider of an interactive computer service may submit STARs under this section.

(2) DESIGNATED AGENCY.—

(A) IN GENERAL.—In carrying out this section, the Attorney General shall designate an agency within the Department, or, if the Attorney General determines appropriate, establish a new agency within the Department, to which STARs should be submitted under subsection (a).

(B) CONSUMER REPORTING.—The agency designated or established under subparagraph (A) shall establish a centralized online resource, which may be used by individual members of the public to report suspicious activity related to major crimes for investigation by the appropriate law enforcement or regulatory agency.

(C) COOPERATION WITH INDUSTRY.—The agency designated or established under subparagraph (A)—

(i) may conduct training for enforcement agencies and for providers of interactive computer services on how to cooperate in reporting suspicious activity;

(ii) may develop relationships for promotion of reporting mechanisms and resources available on the centralized online resource required to be established under subparagraph (B); and

(iii) shall coordinate with the National White Collar Crime Center to convene experts to design training programs for State and local law enforcement agencies, which may include using social media, online ads, paid placements, and partnering with expert non-profit organizations to promote awareness and engage with the public.

(c) CONTENTS.—Each STAR submitted under this section shall contain, at a minimum—

(1) the name, location, and other such identification information as submitted by the user to the provider of the interactive computer service;

(2) the date and nature of the post, message, comment, tag, transaction, or other user-generated content or transmission detected for suspicious activity such as time, origin, and destination; and

(3) any relevant text, information, and metadata related to the suspicious transmission.

(d) RETENTION OF RECORDS AND NONDISCLOSURE.—

(1) RETENTION OF RECORDS.—Each provider of an interactive computer service shall—

(A) maintain a copy of any STAR submitted under this section and the original record equivalent of any supporting documentation for the 5-year period beginning on the date on which the STAR was submitted;

(B) make all supporting documentation available to the Department and any appropriate law enforcement agencies upon request; and

(C) not later than 30 days after the date on which the provider submits a STAR under this section, take action against the website or account reported unless the provider receives a notification from a law enforcement agency that the website or account should remain open.

(2) NONDISCLOSURE.—Except as otherwise prescribed by the Attorney General, no provider of an interactive computer service, or officer, director, employee, or agent of such a provider, subject to an order under subsection (a) may disclose the existence of, or terms of, the order to any person.

(e) DISCLOSURE TO OTHER AGENCIES.—

(1) IN GENERAL.—Subject to paragraph (2), the Attorney General shall—

(A) ensure that STARs submitted under this section and reports from the public submitted under subsection (b)(2)(B) are referred as necessary to the appropriate Federal, State, or local law enforcement or regulatory agency;

(B) make information in a STAR submitted under this section available to an agency, including any State financial institutions supervisory agency or United States intelligence agency, upon request of the head of the agency; and

(C) develop a strategy to disseminate relevant information in a STAR submitted under this section in a timely manner to other law enforcement and government agencies, as appropriate, and coordinate with relevant nongovernmental entities, such as the National Center for Missing and Exploited Children.

(2) LIMITATION.—The Attorney General may only make a STAR available under paragraph (1) for law enforcement purposes.

(f) COMPLIANCE.—Any provider of an interactive computer service that fails to report a known suspicious transmission shall not be immune from civil or criminal liability for such transmission under section 230(c) of the Communications Act of 1934 (47 U.S.C. 230(c)).

(g) APPLICATION OF FOIA.—Any STAR submitted under this section, and any information therein or record thereof, shall be exempt from disclosure under section 552 of title 5, United States Code, or any similar State, local, Tribal, or territorial law.

(h) RULEMAKING AUTHORITY.—Not later than 180 days after the date of enactment of this Act, the Attorney General shall promulgate regulations to carry out this section.

(i) REPORT.—Not later than 180 days after the date of enactment of this Act, the Attorney General shall submit to Congress a report describing the plan of the Department for implementation of this subtitle, including a breakdown of the costs associated with implementation.

(j) AUTHORIZATION OF APPROPRIATIONS.—There are authorized to be appropriated to the Attorney General such sums as may be necessary to carry out this subtitle.

SEC. 1085. AMENDMENT TO COMMUNICATIONS DECENCY ACT.

Section 230(e) of the Communications Act of 1934 (47 U.S.C. 230(e)) is amended by adding at the end the following:

''(6) LOSS OF LIABILITY PROTECTION FOR FAILURE TO SUBMIT SUSPICIOUS TRANSMISSION ACTIVITY REPORT.—

''(A) DEFINITIONS.—In this paragraph, the terms 'known suspicious transmission' and 'suspicious transmission' have the meanings given those terms in section 1083 of the See Something, Say Something Online Act of 2022.

''(B) REQUIREMENT.—Any provider of an interactive computer service shall take reasonable steps to prevent or address unlawful users of the service through the reporting of suspicious transmissions.

''(C) FAILURE TO COMPLY.—Any provider of an interactive computer service that fails to report a known suspicious transmission may be held liable as a publisher for the related suspicious transmission.

''(D) RULE OF CONSTRUCTION.—Nothing in this paragraph shall be construed to impair or limit any claim or cause of action arising from the failure of a provider of an interactive computer service to report a suspicious transmission.''.

SA 6321. Ms. HASSAN (for herself and Mr. CORNYN) submitted an amendment intended to be proposed to amendment SA 5499 submitted by Mr. REED (for himself and Mr. INHOFE) and intended to be proposed to the bill H.R. 7900, to authorize appropriations for fiscal year 2023 for military activities of the Department of Defense, for military construction, and for defense activities of the Department of Energy, to prescribe military personnel strengths for such fiscal year, and for other purposes; which was ordered to lie on the table; as follows:

At the appropriate place, insert the following:

SEC. ___. PILOT PROGRAM ON CYBERSECURITY TRAINING FOR VETERANS AND MILITARY SPOUSES.

(a) DEFINITIONS.—In this section:

(1) EVIDENCE-BASED; WORK-BASED LEARNING.—The terms ''evidence-based'' and ''work-based learning'' have the meanings given those terms in section 3 of the Carl D. Perkins Career and Technical Education Act of 2006 (20 U.S.C. 2302).

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

(3) RECOGNIZED POSTSECONDARY CREDENTIAL.—The term ''recognized postsecondary credential'' has the meaning given the term in section 3 of the Workforce Innovation and Opportunity Act (29 U.S.C. 3102).

(4) REGISTERED APPRENTICESHIP PROGRAM.—The term ''registered apprenticeship program'' means an apprenticeship registered with the Office of Apprenticeship of the Employment and Training Administration of the Department of Labor or a State apprenticeship agency recognized by the Office of the Apprenticeship pursuant to the Act of August 16, 1937 (commonly known as the ''National Apprenticeship Act''; 50 Stat. 664, chapter 663; 29 U.S.C. 50 et seq.)

(5) VETERAN.—The term ''veteran'' has the meaning given the term in section 101 of title 38, United States Code.

(b) ESTABLISHMENT.—Not later than 3 years after the date of enactment of this Act, the Secretary of Homeland Security, in consultation with the Secretary of Veterans Affairs, shall establish a pilot program under which the Secretary of Homeland Security shall provide cybersecurity training to eligible individuals described in subsection (d) at no cost to such individuals.

(c) ELEMENTS.—The cybersecurity training provided under the pilot program established under this section shall be evidence-based and include—

(1) coursework and training that, if applicable, qualifies for postsecondary credit toward an associate, baccalaureate, or graduate degree at an institution of higher education;

(2) virtual learning opportunities;

(3) hands-on learning and performance-based assessments;

(4) Federal work-based learning opportunities and programs (which may include registered apprenticeship programs); and

(5) the provision of recognized postsecondary credentials to eligible individuals who complete the pilot program.

(d) ELIGIBILITY.—

(1) IN GENERAL.—To be eligible for the pilot program under this section, an individual shall be—

(A) a veteran who is entitled to educational assistance under chapter 30, 32, 33, 34, or 35 of title 38, United States Code, or chapter 1606 or 1607 of title 10, United States Code;

(B) a member of an active or a reserve component of the Armed Forces who the Secretary of Homeland Security determines will

become an eligible individual under subparagraph (A) within 180 days of the date of such determination; or

(C) an eligible spouse described in section 1784a(b) of title 10, United States Code.

(2) NO CHARGE TO ENTITLEMENT.—In the case of an individual described in paragraph (1)(A), training under this section shall be provided to the individual without charge to the entitlement of the individual to educational assistance under the laws administered by the Secretary of Veterans Affairs.

(e) ALIGNMENT WITH NICE WORKFORCE FRAMEWORK FOR CYBERSECURITY.—In carrying out the pilot program under this section, the Secretary of Homeland Security shall ensure alignment with the taxonomy, including work roles and competencies and the associated tasks, knowledge, and skills, from the National Initiative for Cybersecurity Education Workforce Framework for Cybersecurity (NIST Special Publication 800–181, Revision 1), or successor framework.

(f) COORDINATION.—

(1) TRAINING, PLATFORMS, AND FRAMEWORKS.—In developing the pilot program under this section, the Secretary of Homeland Security shall coordinate with the Secretary of Veterans Affairs, the Secretary of Defense, the Secretary of Labor, the Secretary of Education, the Director of the National Institute of Standards and Technology, and the Director of the Office of Personnel Management to evaluate and, where possible, leverage existing training, platforms, and frameworks of the Federal Government for providing cybersecurity education and training to prevent duplication of efforts.

(2) FEDERAL WORK-BASED LEARNING OPPORTUNITIES AND PROGRAMS.—In developing the Federal work-based learning opportunities and programs required under subsection (c)(4), the Secretary of Homeland Security shall coordinate with the Secretary of Veterans Affairs, the Secretary of Defense, the Secretary of Labor, the Secretary of Education, the Director of the Office of Personnel Management, and the heads of other appropriate Federal agencies to identify or create, as necessary, interagency opportunities to provide participants in the pilot program with—

(A) opportunities to acquire and demonstrate skills and competencies; and

(B) the capabilities necessary to qualify for Federal employment in a cybersecurity work role.

(g) RESOURCES.—

(1) IN GENERAL.—In any case in which the pilot program—

(A) uses training, platforms, and frameworks described in subsection (f)(1), the Secretary of Homeland Security, in consultation with the Secretary of Veterans Affairs, shall ensure that the trainings, platforms, and frameworks are expanded and resourced to accommodate usage by eligible individuals participating in the pilot program; or

(B) does not use training, platforms, and frameworks described in subsection (f)(1), the Secretary of Homeland Security, in consultation with the Secretary of Veterans Affairs and the heads of other Federal agencies described in subsection (f), shall develop or procure training, platforms, and frameworks necessary to carry out the requirements of subsection (c) and accommodate the usage by eligible individuals participating in the pilot program.

(2) ACTIONS.—In carrying out paragraph (1), the Secretary of Homeland Security may provide additional funding, staff, or other resources to—

(A) recruit and retain women, underrepresented minorities, and individuals from other underrepresented communities;

(B) provide administrative support for basic functions of the pilot program;

(C) ensure the success and ongoing mentoring of eligible individuals participating in the pilot program;

(D) connect participants who complete the pilot program to cybersecurity job opportunities within the Federal Government; and

(E) allocate, if necessary, dedicated positions for term employment to enable Federal work-based learning opportunities and programs, as required under subsection (c)(4), for participants to gain the skills and the competencies necessary to pursue permanent Federal employment in a cybersecurity work role.

(h) REPORTS.—

(1) SECRETARY.—Not later than 2 years after the date on which the pilot program is established under this section, and annually thereafter, the Secretary of Homeland Security shall submit to Congress a report on the pilot program, which shall include—

(A) a description of—

(i) any activity carried out by the Department of Homeland Security under this section; and

(ii) the existing training, platforms, and frameworks of the Federal Government leveraged in accordance with subsection (f)(1); and

(B) an assessment of the results achieved by the pilot program, including—

(i) the admittance rate into the pilot program;

(ii) the employment status of individuals prior to participating in the pilot program, including the sector of employment and type of employer;

(iii) the demographics of participants in the pilot program, including representation of women, underrepresented minorities, and individuals from other underrepresented communities;

(iv) the completion rate for the pilot program, including if there are any identifiable patterns with respect to participants who do not complete the pilot program;

(v) as applicable, the transfer rates to other academic or vocational programs, and certifications and licensure exam passage rates;

(vi) the rate of continued employment within a Federal agency for participants after completing the pilot program;

(vii) the rate of continued employment for participants after completing the pilot program; and

(viii) the median annual salary of participants who completed the pilot program and were subsequently employed, disaggregated by the sector of employment and type of employer and compared to the median annual salary prior to participation in the pilot program.

(2) COMPTROLLER GENERAL.—Not later than 4 years after the date on which the pilot program is established under this section, the Comptroller General of the United States shall submit to Congress a report on the pilot program, including the recommendation of the Comptroller General with respect to whether the pilot program should be extended.

(i) TERMINATION.—The authority to carry out the pilot program under this section shall terminate on the date that is 5 years after the date on which the Secretary of Homeland Security establishes the pilot program under this section.

(j) FEDERAL CYBERSECURITY WORKFORCE ASSESSMENT EXTENSION.—Section 304(a) of the Federal Cybersecurity Workforce Assessment Act of 2015 (5 U.S.C. 301 note) is amended, in the matter preceding paragraph (1), by striking ''2022'' and inserting ''2025''.

SA 6322. Mr. BROWN (for himself and Mr. PORTMAN) submitted an amendment intended to be proposed to amendment SA 5499 submitted by Mr. REED (for himself and Mr. INHOFE) and intended to be proposed to the bill H.R. 7900, to authorize appropriations for fiscal year 2023 for military activities of the Department of Defense, for military construction, and for defense activities of the Department of Energy, to prescribe military personnel strengths for such fiscal year, and for other purposes; which was ordered to lie on the table; as follows:

At the appropriate place in the table in section 4601, under the heading ''Air Force Reserve'', insert the following:

SA 6323. Mr. BROWN (for himself and Mr. PORTMAN) submitted an amendment intended to be proposed to amendment SA 5499 submitted by Mr. REED (for himself and Mr. INHOFE) and intended to be proposed to the bill H.R. 7900, to authorize appropriations for fiscal year 2023 for military activities of the Department of Defense, for military construction, and for defense activities of the Department of Energy, to prescribe military personnel strengths for such fiscal year, and for other purposes; which was ordered to lie on the table; as follows:

At the appropriate place in the table in section 4601, under the heading ''Army National Guard'', insert the following:

SA 6324. Mr. BROWN (for himself and Mr. PORTMAN) submitted an amendment intended to be proposed to amendment SA 5499 submitted by Mr. REED (for himself and Mr. INHOFE) and intended to be proposed to the bill H.R. 7900, to authorize appropriations for fiscal year 2023 for military activities of the Department of Defense, for military construction, and for defense activities of the Department of Energy, to prescribe military personnel strengths for such fiscal year, and for other purposes; which was ordered to lie on the table; as follows:

At the appropriate place in the table in section 4601, under the heading ''Air National Guard'', insert the following:

SA 6325. Mr. BROWN (for himself and Mr. PORTMAN) submitted an amendment intended to be proposed to amendment SA 5499 submitted by Mr. REED (for himself and Mr. INHOFE) and intended to be proposed to the bill H.R. 7900, to authorize appropriations for fiscal year 2023 for military activities of the Department of Defense, for military construction, and for defense activities of the Department of Energy, to prescribe military personnel strengths for such fiscal year, and for other purposes; which was ordered to lie on the table; as follows:

On page 446, between lines 15 and 16, insert the following:

''(c) NATIONAL SPACE INTELLIGENCE CENTER.—

''(1) ESTABLISHMENT.—The Secretary of the Air Force shall establish the National Space Intelligence Center within the Space Force