

AMENDMENT TO RULES COMMITTEE PRINT 117–

13

OFFERED BY MR. THOMPSON OF MISSISSIPPI AND MR. KATKO OF NEW YORK

Insert after title LIII the following new title:

1 **TITLE LIV—DEPARTMENT OF**
2 **HOMELAND SECURITY MEAS-**
3 **URES**

4 **Subtitle A—DHS Headquarters, Re-**
5 **search and Development, and**
6 **Related Matters**

7 **SEC. 5401. CHIEF HUMAN CAPITAL OFFICER RESPONSIBIL-**
8 **ITIES.**

9 Section 704 of the Homeland Security Act of 2002
10 (6 U.S.C. 344) is amended—

11 (1) in subsection (b)—

12 (A) in paragraph (1)—

13 (i) by inserting “, including with re-
14 spect to leader development and employee
15 engagement,” after “policies”;

16 (ii) by striking “and in line” and in-
17 serting “, in line”; and

1 (iii) by inserting “and informed by
2 best practices within the Federal Govern-
3 ment and the private sector,” after “prior-
4 ities,”;

5 (B) in paragraph (2), by striking “develop
6 performance measures to provide a basis for
7 monitoring and evaluating” and inserting “use
8 performance measures to evaluate, on an ongo-
9 ing basis,”;

10 (C) in paragraph (3), by inserting “that,
11 to the extent practicable, are informed by em-
12 ployee feedback” after “policies”;

13 (D) in paragraph (4), by inserting “includ-
14 ing leader development and employee engage-
15 ment programs,” before “in coordination”;

16 (E) in paragraph (5), by inserting before
17 the semicolon at the end the following: “that is
18 informed by an assessment, carried out by the
19 Chief Human Capital Officer, of the learning
20 and developmental needs of employees in super-
21 visory and nonsupervisory roles across the De-
22 partment and appropriate workforce planning
23 initiatives”;

1 (F) by redesignating paragraphs (9) and
2 (10) as paragraphs (13) and (14), respectively;
3 and

4 (G) by inserting after paragraph (8) the
5 following new paragraphs:

6 “(9) maintain a catalogue of available employee
7 development opportunities, including the Homeland
8 Security Rotation Program pursuant to section 844,
9 departmental leadership development programs,
10 interagency development programs, and other rota-
11 tional programs;

12 “(10) ensure that employee discipline and ad-
13 verse action programs comply with the requirements
14 of all pertinent laws, rules, regulations, and Federal
15 guidance, and ensure due process for employees;

16 “(11) analyze each Department or Government-
17 wide Federal workforce satisfaction or morale survey
18 not later than 90 days after the date of the publica-
19 tion of each such survey and submit to the Secretary
20 such analysis, including, as appropriate, rec-
21 ommendations to improve workforce satisfaction or
22 morale within the Department;

23 “(12) review and approve all component em-
24 ployee engagement action plans to ensure such plans
25 include initiatives responsive to the root cause of em-

1 ployee engagement challenges, as well as outcome-
2 based performance measures and targets to track
3 the progress of such initiatives;”;

4 (2) by redesignating subsections (d) and (e) as
5 subsections (e) and (f), respectively;

6 (3) by inserting after subsection (c) the fol-
7 lowing new subsection:

8 “(d) CHIEF LEARNING AND ENGAGEMENT OFFI-
9 CER.—The Chief Human Capital Officer may designate
10 an employee of the Department to serve as a Chief Learn-
11 ing and Engagement Officer to assist the Chief Human
12 Capital Officer in carrying out this section.”; and

13 (4) in subsection (e), as so redesignated—

14 (A) by redesignating paragraphs (2), (3),
15 and (4) as paragraphs (5), (6), and (7), respec-
16 tively; and

17 (B) by inserting after paragraph (1) the
18 following new paragraphs:

19 “(2) information on employee development op-
20 portunities catalogued pursuant to paragraph (9) of
21 subsection (b) and any available data on participa-
22 tion rates, attrition rates, and impacts on retention
23 and employee satisfaction;

1 “(3) information on the progress of Depart-
2 mentwide strategic workforce planning efforts as de-
3 termined under paragraph (2) of subsection (b);

4 “(4) information on the activities of the steer-
5 ing committee established pursuant to section
6 711(a), including the number of meetings, types of
7 materials developed and distributed, and rec-
8 ommendations made to the Secretary;”.

9 **SEC. 5402. EMPLOYEE ENGAGEMENT STEERING COM-**
10 **MITTEE AND ACTION PLAN.**

11 (a) IN GENERAL.—Title VII of the Homeland Secu-
12 rity Act of 2002 (6 U.S.C. 341 et seq.) is amended by
13 adding at the end the following new section:

14 **“SEC. 711. EMPLOYEE ENGAGEMENT.**

15 “(a) STEERING COMMITTEE.—Not later than 120
16 days after the date of the enactment of this section, the
17 Secretary shall establish an employee engagement steering
18 committee, including representatives from operational
19 components, headquarters, and field personnel, including
20 supervisory and nonsupervisory personnel, and employee
21 labor organizations that represent Department employees,
22 and chaired by the Under Secretary for Management, to
23 carry out the following activities:

24 “(1) Identify factors that have a negative im-
25 pact on employee engagement, morale, and commu-

1 nications within the Department, such as percep-
2 tions about limitations on career progression, mobil-
3 ity, or development opportunities, collected through
4 employee feedback platforms, including through an-
5 nual employee surveys, questionnaires, and other
6 communications, as appropriate.

7 “(2) Identify, develop, and distribute initiatives
8 and best practices to improve employee engagement,
9 morale, and communications within the Department,
10 including through annual employee surveys, ques-
11 tionnaires, and other communications, as appro-
12 priate.

13 “(3) Monitor efforts of each component to ad-
14 dress employee engagement, morale, and commu-
15 nications based on employee feedback provided
16 through annual employee surveys, questionnaires,
17 and other communications, as appropriate.

18 “(4) Advise the Secretary on efforts to improve
19 employee engagement, morale, and communications
20 within specific components and across the Depart-
21 ment.

22 “(5) Conduct regular meetings and report, not
23 less than once per quarter, to the Under Secretary
24 for Management, the head of each component, and

1 the Secretary on Departmentwide efforts to improve
2 employee engagement, morale, and communications.

3 “(b) ACTION PLAN; REPORTING.—The Secretary,
4 acting through the Chief Human Capital Officer, shall—

5 “(1) not later than 120 days after the date of
6 the establishment of the employee engagement steer-
7 ing committee under subsection (a), issue a Depart-
8 mentwide employee engagement action plan, reflect-
9 ing input from the steering committee and employee
10 feedback provided through annual employee surveys,
11 questionnaires, and other communications in accord-
12 ance with paragraph (1) of such subsection, to exe-
13 cute strategies to improve employee engagement,
14 morale, and communications within the Department;
15 and

16 “(2) require the head of each component to—

17 “(A) develop and implement a component-
18 specific employee engagement plan to advance
19 the action plan required under paragraph (1)
20 that includes performance measures and objec-
21 tives, is informed by employee feedback pro-
22 vided through annual employee surveys, ques-
23 tionnaires, and other communications, as appro-
24 priate, and sets forth how employees and, where
25 applicable, their labor representatives are to be

1 integrated in developing programs and initia-
2 tives;

3 “(B) monitor progress on implementation
4 of such action plan; and

5 “(C) provide to the Chief Human Capital
6 Officer and the steering committee quarterly re-
7 ports on actions planned and progress made
8 under this paragraph.

9 “(c) NONAPPLICABILITY OF FACA.—The Federal
10 Advisory Committee Act (5 U.S.C. App.) shall not apply
11 to the steering committee and its subcommittees.

12 “(d) TERMINATION.—This section shall terminate on
13 the date that is five years after the date of the enactment
14 of this section.”.

15 (b) CLERICAL AMENDMENT.—The table of contents
16 in section 1(b) of the Homeland Security Act of 2002 is
17 amended by inserting after the item relating to section
18 710 the following new item:

“Sec. 711. Employee engagement.”.

19 (c) SUBMISSIONS TO CONGRESS.—

20 (1) DEPARTMENTWIDE EMPLOYEE ENGAGE-
21 MENT ACTION PLAN.—The Secretary of Homeland
22 Security, acting through the Chief Human Capital
23 Officer of the Department of Homeland Security,
24 shall submit to the Committee on Homeland Secu-
25 rity of the House of Representatives and the Com-

1 mittee on Homeland Security and Governmental Af-
2 fairs of the Senate the Departmentwide employee
3 engagement action plan required under subsection
4 (b)(1) of section 711 of the Homeland Security Act
5 of 2002 (as added by subsection (a) of this section)
6 not later than 30 days after the issuance of such
7 plan under such subsection (b)(1).

8 (2) COMPONENT-SPECIFIC EMPLOYEE ENGAGE-
9 MENT PLANS.—Each head of a component of the
10 Department of Homeland Security shall submit to
11 the Committee on Homeland Security of the House
12 of Representatives and the Committee on Homeland
13 Security and Governmental Affairs of the Senate the
14 component-specific employee engagement plan of
15 each such component required under subsection
16 (b)(2) of section 711 of the Homeland Security Act
17 of 2002 not later than 30 days after the issuance of
18 each such plan under such subsection (b)(2).

19 **SEC. 5403. ANNUAL EMPLOYEE AWARD PROGRAM.**

20 (a) IN GENERAL.—Title VII of the Homeland Secu-
21 rity Act of 2002 (6 U.S.C. 341 et seq.), as amended by
22 section 5302 of this Act, is further amended by adding
23 at the end the following new section:

1 **“SEC. 712. ANNUAL EMPLOYEE AWARD PROGRAM.**

2 “(a) IN GENERAL.—The Secretary may establish an
3 annual employee award program to recognize Department
4 employees or groups of employees for significant contribu-
5 tions to the achievement of the Department’s goals and
6 missions. If such a program is established, the Secretary
7 shall—

8 “(1) establish within such program categories
9 of awards, each with specific criteria, that emphasize
10 honoring employees who are at the nonsupervisory
11 level;

12 “(2) publicize within the Department how any
13 employee or group of employees may be nominated
14 for an award;

15 “(3) establish an internal review board com-
16 prised of representatives from Department compo-
17 nents, headquarters, and field personnel to submit to
18 the Secretary award recommendations regarding
19 specific employees or groups of employees;

20 “(4) select recipients from the pool of nominees
21 submitted by the internal review board under para-
22 graph (3) and convene a ceremony at which employ-
23 ees or groups of employees receive such awards from
24 the Secretary; and

25 “(5) publicize such program within the Depart-
26 ment.

1 “(b) INTERNAL REVIEW BOARD.—The internal re-
2 view board described in subsection (a)(3) shall, when car-
3 rying out its function under such subsection, consult with
4 representatives from operational components and head-
5 quarters, including supervisory and nonsupervisory per-
6 sonnel, and employee labor organizations that represent
7 Department employees.

8 “(c) RULE OF CONSTRUCTION.—Nothing in this sec-
9 tion may be construed to authorize additional funds to
10 carry out the requirements of this section or to require
11 the Secretary to provide monetary bonuses to recipients
12 of an award under this section.”.

13 (b) CLERICAL AMENDMENT.—The table of contents
14 in section 1(b) of the Homeland Security Act of 2002, as
15 amended by section 5402 of this Act, is further amended
16 by inserting after the item relating to section 711 the fol-
17 lowing new item:

“Sec. 712. Annual employee award program.”.

18 **SEC. 5404. INDEPENDENT INVESTIGATION AND IMPLEMEN-**
19 **TATION PLAN.**

20 (a) IN GENERAL.—Not later than 120 days after the
21 date of the enactment of this Act, the Comptroller General
22 of the United States shall investigate whether the applica-
23 tion in the Department of Homeland Security of discipline
24 and adverse actions are administered in an equitable and
25 consistent manner that results in the same or substantially

1 similar disciplinary outcomes across the Department for
2 misconduct by a nonsupervisory or supervisor employee
3 who engaged in the same or substantially similar mis-
4 conduct.

5 (b) CONSULTATION.—In carrying out the investiga-
6 tion described in subsection (a), the Comptroller General
7 of the United States shall consult with the Under Sec-
8 retary for Management of the Department of Homeland
9 Security and the employee engagement steering committee
10 established pursuant to subsection (b)(1) of section 711
11 of the Homeland Security Act of 2002 (as added by sec-
12 tion 5302(a) of this Act).

13 (c) ACTION BY UNDER SECRETARY FOR MANAGE-
14 MENT.—Upon completion of the investigation described in
15 subsection (a), the Under Secretary for Management of
16 the Department of Homeland Security shall review the
17 findings and recommendations of such investigation and
18 implement a plan, in consultation with the employee en-
19 gagement steering committee established pursuant to sub-
20 section (b)(1) of section 711 of the Homeland Security
21 Act of 2002, to correct any relevant deficiencies identified
22 by the Comptroller General of the United States in such
23 investigation. The Under Secretary for Management shall
24 direct the employee engagement steering committee to re-

1 view such plan to inform committee activities and action
2 plans authorized under such section 711.

3 **SEC. 5405. IMPACTS OF SHUTDOWN.**

4 Not later than 90 days after the date of the enact-
5 ment of this Act, the Secretary of Homeland Security shall
6 report to the Committee on Homeland Security of the
7 House of Representatives and the Committee on Home-
8 land Security and Governmental Affairs of the Senate re-
9 garding the direct and indirect impacts of the lapse in ap-
10 propriations between December 22, 2018, and January
11 25, 2019, on—

12 (1) Department of Homeland Security human
13 resources operations;

14 (2) the Department's ability to meet hiring
15 benchmarks; and

16 (3) retention, attrition, and morale of Depart-
17 ment personnel.

18 **SEC. 5406. TECHNICAL CORRECTIONS TO QUADRENNIAL**
19 **HOMELAND SECURITY REVIEW.**

20 (a) IN GENERAL.—Section 707 of the Homeland Se-
21 curity Act of 2002 (6 U.S.C. 347) is amended—

22 (1) in subsection (a)(3)—

23 (A) in subparagraph (B), by striking
24 “and” after the semicolon at the end;

1 (B) by redesignating subparagraph (C) as
2 subparagraph (D); and

3 (C) by inserting after subparagraph (B)
4 the following new subparagraph:

5 “(C) representatives from appropriate ad-
6 visory committees established pursuant to sec-
7 tion 871, including the Homeland Security Ad-
8 visory Council and the Homeland Security
9 Science and Technology Advisory Committee, or
10 otherwise established, including the Aviation
11 Security Advisory Committee established pursu-
12 ant to section 44946 of title 49, United States
13 Code; and”;

14 (2) in subsection (b)—

15 (A) in paragraph (2), by inserting before
16 the semicolon at the end the following: “based
17 on the risk assessment required pursuant to
18 subsection (c)(2)(B)”;

19 (B) in paragraph (3)—

20 (i) by inserting “, to the extent prac-
21 ticable,” after “describe”; and

22 (ii) by striking “budget plan” and in-
23 serting “resources required”;

24 (C) in paragraph (4)—

1 (i) by inserting “, to the extent prac-
2 ticable,” after “identify”;

3 (ii) by striking “budget plan required
4 to provide sufficient resources to success-
5 fully” and inserting “resources required
6 to”; and

7 (iii) by striking the semicolon at the
8 end and inserting the following: “, includ-
9 ing any resources identified from redun-
10 dant, wasteful, or unnecessary capabilities
11 or capacities that may be redirected to bet-
12 ter support other existing capabilities or
13 capacities, as the case may be; and”;

14 (D) in paragraph (5), by striking “; and”
15 and inserting a period; and

16 (E) by striking paragraph (6);

17 (3) in subsection (c)—

18 (A) in paragraph (1), by striking “Decem-
19 ber 31 of the year” and inserting “60 days
20 after the date of the submission of the Presi-
21 dent’s budget for the fiscal year after the fiscal
22 year”;

23 (B) in paragraph (2)—

1 (i) in subparagraph (B), by striking
2 “description of the threats to” and insert-
3 ing “risk assessment of”;

4 (ii) in subparagraph (C), by inserting
5 “, as required under subsection (b)(2)” be-
6 fore the semicolon at the end;

7 (iii) in subparagraph (D)—

8 (I) by inserting “to the extent
9 practicable,” before “a description”;
10 and

11 (II) by striking “budget plan”
12 and inserting “resources required”;

13 (iv) in subparagraph (F)—

14 (I) by inserting “to the extent
15 practicable,” before “a discussion”;
16 and

17 (II) by striking “the status of”;

18 (v) in subparagraph (G)—

19 (I) by inserting “to the extent
20 practicable,” before “a discussion”;

21 (II) by striking “the status of”;

22 (III) by inserting “and risks” be-
23 fore “to national homeland”; and

24 (IV) by inserting “and” after the
25 semicolon at the end;

1 (vi) by striking subparagraph (H);

2 and

3 (vii) by redesignating subparagraph

4 (I) as subparagraph (H);

5 (C) by redesignating paragraph (3) as
6 paragraph (4); and

7 (D) by inserting after paragraph (2) the
8 following new paragraph:

9 “(3) DOCUMENTATION.—The Secretary shall
10 retain and, upon request, provide to Congress the
11 following documentation regarding each quadrennial
12 homeland security review:

13 “(A) Records regarding the consultation
14 carried out pursuant to subsection (a)(3), in-
15 cluding the following:

16 “(i) All written communications, in-
17 cluding communications sent out by the
18 Secretary and feedback submitted to the
19 Secretary through technology, online com-
20 munications tools, in-person discussions,
21 and the interagency process.

22 “(ii) Information on how feedback re-
23 ceived by the Secretary informed each such
24 quadrennial homeland security review.

1 “(B) Information regarding the risk as-
2 sessment required pursuant to subsection
3 (c)(2)(B), including the following:

4 “(i) The risk model utilized to gen-
5 erate such risk assessment.

6 “(ii) Information, including data used
7 in the risk model, utilized to generate such
8 risk assessment.

9 “(iii) Sources of information, includ-
10 ing other risk assessments, utilized to gen-
11 erate such risk assessment.

12 “(iv) Information on assumptions,
13 weighing factors, and subjective judgments
14 utilized to generate such risk assessment,
15 together with information on the rationale
16 or basis thereof.”;

17 (4) by redesignating subsection (d) as sub-
18 section (e); and

19 (5) by inserting after subsection (c) the fol-
20 lowing new subsection:

21 “(d) REVIEW.—Not later than 90 days after the sub-
22 mission of each report required under subsection (c)(1),
23 the Secretary shall provide to the Committee on Homeland
24 Security of the House of Representatives and the Com-
25 mittee on Homeland Security and Governmental Affairs

1 of the Senate information on the degree to which the find-
2 ings and recommendations developed in the quadrennial
3 homeland security review that is the subject of such report
4 were integrated into the acquisition strategy and expendi-
5 ture plans for the Department.”.

6 (b) EFFECTIVE DATE.—The amendments made by
7 this section shall apply with respect to a quadrennial
8 homeland security review conducted after December 31,
9 2021.

10 **SEC. 5407. AUTHORIZATION OF THE ACQUISITION PROFES-**
11 **SIONAL CAREER PROGRAM.**

12 (a) IN GENERAL.—Title VII of the Homeland Secu-
13 rity Act of 2002 (6 U.S.C. 341 et seq.), as amended by
14 section 5304 of this Act, is further amended by adding
15 at the end the following new section:

16 **“SEC. 713. ACQUISITION PROFESSIONAL CAREER PRO-**
17 **GRAM.**

18 “(a) ESTABLISHMENT.—There is established in the
19 Department an acquisition professional career program to
20 develop a cadre of acquisition professionals within the De-
21 partment.

22 “(b) ADMINISTRATION.—The Under Secretary for
23 Management shall administer the acquisition professional
24 career program established pursuant to subsection (a).

1 “(c) PROGRAM REQUIREMENTS.—The Under Sec-
2 retary for Management shall carry out the following with
3 respect to the acquisition professional career program.

4 “(1) Designate the occupational series, grades,
5 and number of acquisition positions throughout the
6 Department to be included in the program and man-
7 age centrally such positions.

8 “(2) Establish and publish on the Department’s
9 website eligibility criteria for candidates to partici-
10 pate in the program.

11 “(3) Carry out recruitment efforts to attract
12 candidates—

13 “(A) from institutions of higher education,
14 including such institutions with established ac-
15 quisition specialties and courses of study, his-
16 torically Black colleges and universities, and
17 Hispanic-serving institutions;

18 “(B) with diverse work experience outside
19 of the Federal Government; or

20 “(C) with military service.

21 “(4) Hire eligible candidates for designated po-
22 sitions under the program.

23 “(5) Develop a structured program comprised
24 of acquisition training, on-the-job experience, De-
25 partmentwide rotations, mentorship, shadowing, and

1 other career development opportunities for program
2 participants.

3 “(6) Provide, beyond required training estab-
4 lished for program participants, additional special-
5 ized acquisition training, including small business
6 contracting and innovative acquisition techniques
7 training.

8 “(d) REPORTS.—Not later than December 31, 2021,
9 and annually thereafter through 2027, the Secretary shall
10 submit to the Committee on Homeland Security of the
11 House of Representatives and the Committee on Home-
12 land Security and Governmental Affairs of the Senate a
13 report on the acquisition professional career program.
14 Each such report shall include the following information:

15 “(1) The number of candidates approved for
16 the program.

17 “(2) The number of candidates who commenced
18 participation in the program, including generalized
19 information on such candidates’ backgrounds with
20 respect to education and prior work experience, but
21 not including personally identifiable information.

22 “(3) A breakdown of the number of partici-
23 pants hired under the program by type of acquisition
24 position.

1 “(4) A list of Department components and of-
2 fices that participated in the program and informa-
3 tion regarding length of time of each program par-
4 ticipant in each rotation at such components or of-
5 fices.

6 “(5) Program attrition rates and postprogram
7 graduation retention data, including information on
8 how such data compare to the prior year’s data, as
9 available.

10 “(6) The Department’s recruiting efforts for
11 the program.

12 “(7) The Department’s efforts to promote re-
13 tention of program participants.

14 “(e) DEFINITIONS.—In this section:

15 “(1) HISPANIC-SERVING INSTITUTION.—The
16 term ‘Hispanic-serving institution’ has the meaning
17 given such term in section 502 of the Higher Edu-
18 cation Act of 1965 (20 U.S.C. 1101a).

19 “(2) HISTORICALLY BLACK COLLEGES AND
20 UNIVERSITIES.—The term ‘historically Black col-
21 leges and universities’ has the meaning given the
22 term ‘part B institution’ in section 322(2) of Higher
23 Education Act of 1965 (20 U.S.C. 1061(2)).

24 “(3) INSTITUTION OF HIGHER EDUCATION.—
25 The term ‘institution of higher education’ has the

1 meaning given such term in section 101 of the High-
2 er Education Act of 1965 (20 U.S.C. 1001).”.

3 (b) CLERICAL AMENDMENT.—The table of contents
4 in section 1(b) of the Homeland Security Act of 2002, as
5 amended by section 5403 of this Act, is further amended
6 by inserting after the item relating to section 712 the fol-
7 lowing new item:

“Sec. 713. Acquisition professional career program.”.

8 **SEC. 5408. NATIONAL URBAN SECURITY TECHNOLOGY LAB-**
9 **ORATORY.**

10 (a) IN GENERAL.—Title III of the Homeland Secu-
11 rity Act of 2002 (6 U.S.C. 181 et seq.) is amended by
12 adding at the end the following new section:

13 **“SEC. 322. NATIONAL URBAN SECURITY TECHNOLOGY LAB-**
14 **ORATORY.**

15 “(a) IN GENERAL.—The Secretary, acting through
16 the Under Secretary for Science and Technology, shall
17 designate the laboratory described in subsection (b) as an
18 additional laboratory pursuant to the authority under sec-
19 tion 308(c)(2). Such laboratory shall be used to test and
20 evaluate emerging technologies and conduct research and
21 development to assist emergency response providers in
22 preparing for, and protecting against, threats of terrorism.

23 “(b) LABORATORY DESCRIBED.—The laboratory de-
24 scribed in this subsection is the laboratory—

1 “(1) known, as of the date of the enactment of
2 this section, as the National Urban Security Tech-
3 nology Laboratory; and

4 “(2) transferred to the Department pursuant to
5 section 303(1)(E).

6 “(c) LABORATORY ACTIVITIES.—The National Urban
7 Security Technology Laboratory shall—

8 “(1) conduct tests, evaluations, and assess-
9 ments of current and emerging technologies, includ-
10 ing, as appropriate, the cybersecurity of such tech-
11 nologies that can connect to the internet, for emer-
12 gency response providers;

13 “(2) act as a technical advisor to emergency re-
14 sponse providers; and

15 “(3) carry out other such activities as the Sec-
16 retary determines appropriate.

17 “(d) RULE OF CONSTRUCTION.—Nothing in this sec-
18 tion may be construed as affecting in any manner the au-
19 thorities or responsibilities of the Countering Weapons of
20 Mass Destruction Office of the Department.”.

21 (b) CLERICAL AMENDMENT.—The table of contents
22 in section 1(b) of the Homeland Security Act of 2002, as
23 amended by section 5407 of this Act, is further amended
24 by inserting after the item relating to section 321 the fol-
25 lowing new item:

“Sec. 322. National Urban Security Technology Laboratory.”.

1 **SEC. 5409. DEPARTMENT OF HOMELAND SECURITY BLUE**
2 **CAMPAIGN ENHANCEMENT.**

3 Section 434 of the Homeland Security Act of 2002
4 (6 U.S.C. 242) is amended—

5 (1) in subsection (e)(6), by striking “utilizing
6 resources,” and inserting “developing and utilizing,
7 in consultation with the Advisory Board established
8 pursuant to subsection (g), resources”; and

9 (2) by adding at the end the following new sub-
10 sections:

11 “(f) **WEB-BASED TRAINING PROGRAMS.**—To en-
12 hance training opportunities, the Director of the Blue
13 Campaign shall develop web-based interactive training vid-
14 eos that utilize a learning management system to provide
15 online training opportunities that shall be made available
16 to the following individuals:

17 “(1) Federal, State, local, Tribal, and territorial
18 law enforcement officers.

19 “(2) Non-Federal correction system personnel.

20 “(3) Such other individuals as the Director de-
21 termines appropriate.

22 “(g) **BLUE CAMPAIGN ADVISORY BOARD.**—

23 “(1) **IN GENERAL.**—The Secretary shall estab-
24 lish within the Department a Blue Campaign Advi-
25 sory Board and shall assign to such Board a rep-
26 resentative from each of the following components:

1 “(A) The Transportation Security Admin-
2 istration.

3 “(B) U.S. Customs and Border Protection.

4 “(C) U.S. Immigration and Customs En-
5 forcement.

6 “(D) The Federal Law Enforcement
7 Training Center.

8 “(E) The United States Secret Service.

9 “(F) The Office for Civil Rights and Civil
10 Liberties.

11 “(G) The Privacy Office.

12 “(H) Any other components or offices the
13 Secretary determines appropriate.

14 “(2) CHARTER.—The Secretary is authorized to
15 issue a charter for the Board, and such charter shall
16 specify the following:

17 “(A) The Board’s mission, goals, and
18 scope of its activities.

19 “(B) The duties of the Board’s representa-
20 tives.

21 “(C) The frequency of the Board’s meet-
22 ings.

23 “(3) CONSULTATION.—The Director shall con-
24 sult the Board established pursuant to paragraph
25 (1) regarding the following:

1 “(A) Recruitment tactics used by human
2 traffickers to inform the development of train-
3 ing and materials by the Blue Campaign.

4 “(B) The development of effective aware-
5 ness tools for distribution to Federal and non-
6 Federal officials to identify and prevent in-
7 stances of human trafficking.

8 “(C) Identification of additional persons or
9 entities that may be uniquely positioned to rec-
10 ognize signs of human trafficking and the devel-
11 opment of materials for such persons.

12 “(4) APPLICABILITY.—The Federal Advisory
13 Committee Act (5 U.S.C. App.) does not apply to—

14 “(A) the Board; or

15 “(B) consultations under paragraph (2).

16 “(h) CONSULTATION.—With regard to the develop-
17 ment of programs under the Blue Campaign and the im-
18 plementation of such programs, the Director is authorized
19 to consult with State, local, Tribal, and territorial agen-
20 cies, nongovernmental organizations, private sector orga-
21 nizations, and experts. Such consultation shall be exempt
22 from the Federal Advisory Committee Act (5 U.S.C.
23 App.).”.

1 **SEC. 5410. DEPARTMENT OF HOMELAND SECURITY MEN-**
2 **TOR-PROTÉGÉ PROGRAM.**

3 (a) IN GENERAL.—Subtitle H of title VIII of the
4 Homeland Security Act of 2002 (6 U.S.C. 451 et seq.)
5 is amended by adding at the end the following new section:

6 **“SEC. 890B. MENTOR-PROTÉGÉ PROGRAM.**

7 “(a) ESTABLISHMENT.—There is established in the
8 Department a mentor-protégé program (in this section re-
9 ferred to as the ‘Program’) under which a mentor firm
10 enters into an agreement with a protégé firm for the pur-
11 pose of assisting the protégé firm to compete for prime
12 contracts and subcontracts of the Department.

13 “(b) ELIGIBILITY.—The Secretary shall establish cri-
14 teria for mentor firms and protégé firms to be eligible to
15 participate in the Program, including a requirement that
16 a firm is not included on any list maintained by the Fed-
17 eral Government of contractors that have been suspended
18 or debarred.

19 “(c) PROGRAM APPLICATION AND APPROVAL.—

20 “(1) APPLICATION.—The Secretary, acting
21 through the Office of Small and Disadvantaged
22 Business Utilization of the Department, shall estab-
23 lish a process for submission of an application joint-
24 ly by a mentor firm and the protégé firm selected by
25 the mentor firm. The application shall include each
26 of the following:

1 “(A) A description of the assistance to be
2 provided by the mentor firm, including, to the
3 extent available, the number and a brief de-
4 scription of each anticipated subcontract to be
5 awarded to the protégé firm.

6 “(B) A schedule with milestones for
7 achieving the assistance to be provided over the
8 period of participation in the Program.

9 “(C) An estimate of the costs to be in-
10 curred by the mentor firm for providing assist-
11 ance under the Program.

12 “(D) Attestations that Program partici-
13 pants will submit to the Secretary reports at
14 times specified by the Secretary to assist the
15 Secretary in evaluating the protégé firm’s devel-
16 opmental progress.

17 “(E) Attestations that Program partici-
18 pants will inform the Secretary in the event of
19 a change in eligibility or voluntary withdrawal
20 from the Program.

21 “(2) APPROVAL.—Not later than 60 days after
22 receipt of an application pursuant to paragraph (1),
23 the head of the Office of Small and Disadvantaged
24 Business Utilization shall notify applicants of ap-

1 proval or, in the case of disapproval, the process for
2 resubmitting an application for reconsideration.

3 “(3) RESCISSION.—The head of the Office of
4 Small and Disadvantaged Business Utilization may
5 rescind the approval of an application under this
6 subsection if it determines that such action is in the
7 best interest of the Department.

8 “(d) PROGRAM DURATION.—A mentor firm and
9 protégé firm approved under subsection (c) shall enter into
10 an agreement to participate in the Program for a period
11 of not less than 36 months.

12 “(e) PROGRAM BENEFITS.—A mentor firm and
13 protégé firm that enter into an agreement under sub-
14 section (d) may receive the following Program benefits:

15 “(1) With respect to an award of a contract
16 that requires a subcontracting plan, a mentor firm
17 may receive evaluation credit for participating in the
18 Program.

19 “(2) With respect to an award of a contract
20 that requires a subcontracting plan, a mentor firm
21 may receive credit for a protégé firm performing as
22 a first-tier subcontractor or a subcontractor at any
23 tier in an amount equal to the total dollar value of
24 any subcontracts awarded to such protégé firm.

1 “(3) A protégé firm may receive technical, man-
2 agerial, financial, or any other mutually agreed upon
3 benefit from a mentor firm, including a subcontract
4 award.

5 “(f) REPORTING.—Not later than one year after the
6 date of the enactment of this Act, and annually thereafter,
7 the head of the Office of Small and Disadvantaged Busi-
8 ness Utilization shall submit to the Committee on Home-
9 land Security and Governmental Affairs and the Com-
10 mittee on Small Business and Entrepreneurship of the
11 Senate and the Committee on Homeland Security and the
12 Committee on Small Business of the House of Representa-
13 tives a report that—

14 “(1) identifies each agreement between a men-
15 tor firm and a protégé firm entered into under this
16 section, including the number of protégé firm par-
17 ticipants that are—

18 “(A) small business concerns;

19 “(B) small business concerns owned and
20 controlled by veterans;

21 “(C) small business concerns owned and
22 controlled by service-disabled veterans;

23 “(D) qualified HUBZone small business
24 concerns;

1 “(E) small business concerns owned and
2 controlled by socially and economically dis-
3 advantaged individuals;

4 “(F) small business concerns owned and
5 controlled by women;

6 “(G) historically Black colleges and univer-
7 sities; and

8 “(H) minority institutions of higher edu-
9 cation;

10 “(2) describes the type of assistance provided
11 by mentor firms to protégé firms;

12 “(3) identifies contracts within the Department
13 in which a mentor firm serving as the prime con-
14 tractor provided subcontracts to a protégé firm
15 under the Program; and

16 “(4) assesses the degree to which there has
17 been—

18 “(A) an increase in the technical capabili-
19 ties of protégé firms; and

20 “(B) an increase in the quantity and esti-
21 mated value of prime contract and subcontract
22 awards to protégé firms for the period covered
23 by the report.

24 “(g) RULE OF CONSTRUCTION.—Nothing in this sec-
25 tion may be construed to limit, diminish, impair, or other-

1 wise affect the authority of the Department to participate
2 in any program carried out by or requiring approval of
3 the Small Business Administration or adopt or follow any
4 regulation or policy that the Administrator of the Small
5 Business Administration may promulgate, except that, to
6 the extent that any provision of this section (including
7 subsection (h)) conflicts with any other provision of law,
8 regulation, or policy, this section shall control.

9 “(h) DEFINITIONS.—In this section:

10 “(1) HISTORICALLY BLACK COLLEGE OR UNI-
11 VERSITY.—The term ‘historically Black college or
12 university’ means any of the historically Black col-
13 leges and universities referred to in section 2323 of
14 title 10, United States Code, as in effect on March
15 1, 2018.

16 “(2) MENTOR FIRM.—The term ‘mentor firm’
17 means a for-profit business concern that is not a
18 small business concern that—

19 “(A) has the ability to assist and commits
20 to assisting a protégé firm to compete for Fed-
21 eral prime contracts and subcontracts; and

22 “(B) satisfies any other requirements im-
23 posed by the Secretary.

24 “(3) MINORITY INSTITUTION OF HIGHER EDU-
25 CATION.—The term ‘minority institution of higher

1 education’ means an institution of higher education
2 with a student body that reflects the composition
3 specified in section 312(b) of the Higher Education
4 Act of 1965 (20 U.S.C. 1058(b)).

5 “(4) PROTÉGÉ FIRM.—The term ‘protégé firm’
6 means a small business concern, a historically Black
7 college or university, or a minority institution of
8 higher education that—

9 “(A) is eligible to enter into a prime con-
10 tract or subcontract with the Department; and

11 “(B) satisfies any other requirements im-
12 posed by the Secretary.

13 “(5) SMALL BUSINESS ACT DEFINITIONS.—The
14 terms ‘small business concern’, ‘small business con-
15 cern owned and controlled by veterans’, ‘small busi-
16 ness concern owned and controlled by service-dis-
17 abled veterans’, ‘qualified HUBZone small business
18 concern’, and ‘small business concern owned and
19 controlled by women’ have the meanings given such
20 terms, respectively, under section 3 of the Small
21 Business Act (15 U.S.C. 632). The term ‘small busi-
22 ness concern owned and controlled by socially and
23 economically disadvantaged individuals’ has the
24 meaning given such term in section 8(d)(3)(C) of
25 the Small Business Act (15 U.S.C. 637(d)(3)(C)).”.

1 (b) CLERICAL AMENDMENT.—The table of contents
2 in section 1(b) of the Homeland Security Act of 2002, as
3 amended by section 5408 of this Act, is further amended
4 by inserting after the item relating to section 890A the
5 following new item:

“Sec. 890B. Mentor-protégé program.”.

6 **SEC. 5411. MEDICAL COUNTERMEASURES PROGRAM.**

7 (a) IN GENERAL.—Subtitle C of title XIX of the
8 Homeland Security Act of 2002 (6 U.S.C. 311 et seq.)
9 is amended by adding at the end the following new section:

10 **“SEC. 1932. MEDICAL COUNTERMEASURES.**

11 “(a) IN GENERAL.—The Secretary shall establish a
12 medical countermeasures program to facilitate personnel
13 readiness, and protection for the Department’s employees
14 and working animals in the event of a chemical, biological,
15 radiological, nuclear, or explosives attack, naturally occur-
16 ring disease outbreak, or pandemic, and to support De-
17 partment mission continuity.

18 “(b) OVERSIGHT.—The Chief Medical Officer of the
19 Department shall provide programmatic oversight of the
20 medical countermeasures program established pursuant to
21 subsection (a), and shall—

22 “(1) develop Departmentwide standards for
23 medical countermeasure storage, security, dis-
24 pensing, and documentation;

1 “(2) maintain a stockpile of medical counter-
2 measures, including antibiotics, antivirals, and radio-
3 logical countermeasures, as appropriate;

4 “(3) preposition appropriate medical counter-
5 measures in strategic locations nationwide, based on
6 threat and employee density, in accordance with ap-
7 plicable Federal statutes and regulations;

8 “(4) provide oversight and guidance regarding
9 the dispensing of stockpiled medical counter-
10 measures;

11 “(5) ensure rapid deployment and dispensing of
12 medical countermeasures in a chemical, biological,
13 radiological, nuclear, or explosives attack, naturally
14 occurring disease outbreak, or pandemic;

15 “(6) provide training to Department employees
16 on medical countermeasure dispensing; and

17 “(7) support dispensing exercises.

18 “(c) MEDICAL COUNTERMEASURES WORKING
19 GROUP.—The Chief Medical Officer shall establish a med-
20 ical countermeasures working group comprised of rep-
21 resentatives from appropriate components and offices of
22 the Department to ensure that medical countermeasures
23 standards are maintained and guidance is consistent.

24 “(d) MEDICAL COUNTERMEASURES MANAGE-
25 MENT.—Not later than 120 days after the date of the en-

1 actment of this section, the Chief Medical Officer shall de-
2 velop and submit to the Secretary an integrated logistics
3 support plan for medical countermeasures, including—

4 “(1) a methodology for determining the ideal
5 types and quantities of medical countermeasures to
6 stockpile and how frequently such methodology shall
7 be reevaluated;

8 “(2) a replenishment plan; and

9 “(3) inventory tracking, reporting, and rec-
10 onciliation procedures for existing stockpiles and
11 new medical countermeasure purchases.

12 “(e) STOCKPILE ELEMENTS.—In determining the
13 types and quantities of medical countermeasures to stock-
14 pile under subsection (d), the Chief Medical Officer shall
15 utilize, if available—

16 “(1) Department chemical, biological, radio-
17 logical, and nuclear risk assessments; and

18 “(2) Centers for Disease Control and Preven-
19 tion guidance on medical countermeasures.

20 “(f) REPORT.—Not later than 180 days after the
21 date of the enactment of this section, the Secretary shall
22 submit to the Committee on Homeland Security of the
23 House of Representatives and the Committee on Home-
24 land Security and Governmental Affairs of the Senate the
25 plan developed in accordance with subsection (d) and brief

1 such Committees regarding implementing the require-
2 ments of this section.

3 “(g) DEFINITION.—In this section, the term ‘medical
4 countermeasures’ means antibiotics, antivirals, radio-
5 logical countermeasures, and other countermeasures that
6 may be deployed to protect the Department’s employees
7 and working animals in the event of a chemical, biological,
8 radiological, nuclear, or explosives attack, naturally occur-
9 ring disease outbreak, or pandemic.”.

10 (b) CLERICAL AMENDMENT.—The table of contents
11 in section 1(b) of the Homeland Security Act of 2002, as
12 amended by section 5410 of this Act, is further amended
13 by inserting after the item relating to section 1931 the
14 following new item:

“Sec. 1932. Medical countermeasures.”.

15 **SEC. 5412. CRITICAL DOMAIN RESEARCH AND DEVELOP-**
16 **MENT.**

17 (a) IN GENERAL.—Subtitle H of title VIII of the
18 Homeland Security Act of 2002 (6 U.S.C. 451 et seq.),
19 as amended by section 5310 of this Act, is further amend-
20 ed by adding at the end the following new section:

21 **“SEC. 890C. HOMELAND SECURITY CRITICAL DOMAIN RE-**
22 **SEARCH AND DEVELOPMENT.**

23 “(a) IN GENERAL.—

1 “(1) RESEARCH AND DEVELOPMENT.—The
2 Secretary is authorized to conduct research and de-
3 velopment to—

4 “(A) identify United States critical do-
5 mains for economic security and homeland se-
6 curity; and

7 “(B) evaluate the extent to which disrup-
8 tion, corruption, exploitation, or dysfunction of
9 any of such domain poses a substantial threat
10 to homeland security.

11 “(2) REQUIREMENTS.—

12 “(A) RISK ANALYSIS OF CRITICAL DO-
13 MAINS.—The research under paragraph (1)
14 shall include a risk analysis of each identified
15 United States critical domain for economic se-
16 curity to determine the degree to which there
17 exists a present or future threat to homeland
18 security in the event of disruption, corruption,
19 exploitation, or dysfunction to such domain.
20 Such research shall consider, to the extent pos-
21 sible, the following:

22 “(i) The vulnerability and resilience of
23 relevant supply chains.

24 “(ii) Foreign production, processing,
25 and manufacturing methods.

1 “(iii) Influence of malign economic ac-
2 tors.

3 “(iv) Asset ownership.

4 “(v) Relationships within the supply
5 chains of such domains.

6 “(vi) The degree to which the condi-
7 tions referred to in clauses (i) through (v)
8 would place such a domain at risk of dis-
9 ruption, corruption, exploitation, or dys-
10 function.

11 “(B) ADDITIONAL RESEARCH INTO HIGH-
12 RISK CRITICAL DOMAINS.—Based on the identi-
13 fication and risk analysis of United States crit-
14 ical domains for economic security pursuant to
15 paragraph (1) and subparagraph (A) of this
16 paragraph, respectively, the Secretary may con-
17 duct additional research into those critical do-
18 mains, or specific elements thereof, with respect
19 to which there exists the highest degree of a
20 present or future threat to homeland security in
21 the event of disruption, corruption, exploitation,
22 or dysfunction to such a domain. For each such
23 high-risk domain, or element thereof, such re-
24 search shall—

1 “(i) describe the underlying infra-
2 structure and processes;

3 “(ii) analyze present and projected
4 performance of industries that comprise or
5 support such domain;

6 “(iii) examine the extent to which the
7 supply chain of a product or service nec-
8 essary to such domain is concentrated, ei-
9 ther through a small number of sources, or
10 if multiple sources are concentrated in one
11 geographic area;

12 “(iv) examine the extent to which the
13 demand for supplies of goods and services
14 of such industries can be fulfilled by
15 present and projected performance of other
16 industries, identify strategies, plans, and
17 potential barriers to expand the supplier
18 industrial base, and identify the barriers to
19 the participation of such other industries;

20 “(v) consider each such domain’s per-
21 formance capacities in stable economic en-
22 vironments, adversarial supply conditions,
23 and under crisis economic constraints;

1 “(vi) identify and define needs and re-
2 quirements to establish supply resiliency
3 within each such domain; and

4 “(vii) consider the effects of sector
5 consolidation, including foreign consolida-
6 tion, either through mergers or acquisi-
7 tions, or due to recent geographic realign-
8 ment, on such industries’ performances.

9 “(3) CONSULTATION.—In conducting the re-
10 search under paragraph (1) and subparagraph (B)
11 of paragraph (2), the Secretary may consult with
12 appropriate Federal agencies, State agencies, and
13 private sector stakeholders.

14 “(4) PUBLICATION.—Beginning one year after
15 the date of the enactment of this section, the Sec-
16 retary shall publish a report containing information
17 relating to the research under paragraph (1) and
18 subparagraph (B) of paragraph (2), including find-
19 ings, evidence, analysis, and recommendations. Such
20 report shall be updated annually through 2026.

21 “(b) SUBMISSION TO CONGRESS.—Not later than 90
22 days after the publication of each report required under
23 paragraph (4) of subsection (a), the Secretary shall trans-
24 mit to the Committee on Homeland Security of the House
25 of Representatives and the Committee on Homeland Secu-

1 rity and Governmental Affairs of the Senate each such re-
2 port, together with a description of actions the Secretary,
3 in consultation with appropriate Federal agencies, will un-
4 dertake or has undertaken in response to each such report.

5 “(c) DEFINITIONS.—In this section:

6 “(1) UNITED STATES CRITICAL DOMAINS FOR
7 ECONOMIC SECURITY.—The term ‘United States
8 critical domains for economic security’ means the
9 critical infrastructure and other associated indus-
10 tries, technologies, and intellectual property, or any
11 combination thereof, that are essential to the eco-
12 nomic security of the United States.

13 “(2) ECONOMIC SECURITY.—The term ‘eco-
14 nomic security’ means the condition of having secure
15 and resilient domestic production capacity, combined
16 with reliable access to the global resources necessary
17 to maintain an acceptable standard of living and to
18 protect core national values.

19 “(d) AUTHORIZATION OF APPROPRIATIONS.—There
20 is authorized to be appropriated \$1,000,000 for each of
21 fiscal years 2022 through 2026 to carry out this section.”.

22 (b) CLERICAL AMENDMENT.—The table of contents
23 in section 1(b) of the Homeland Security Act of 2002, as
24 amended by section 5411 of this Act, is further amended

1 by inserting after the item relating to section 890B the
2 following new item:

“Sec. 890C. Homeland security critical domain research and development.”.

3 **Subtitle B—Cybersecurity**

4 **SEC. 5421. TITLE XXII TECHNICAL AND CLERICAL AMEND-**
5 **MENTS.**

6 (a) TECHNICAL AMENDMENTS.—

7 (1) HOMELAND SECURITY ACT OF 2002.—Sub-
8 title A of title XXII of the Homeland Security Act
9 of 2002 (6 U.S.C. 651 et seq.) is amended—

10 (A) in the first section 2215 (6 U.S.C.
11 665; relating to the duties and authorities relat-
12 ing to .gov internet domain), by amending the
13 section enumerator and heading to read as fol-
14 lows:

15 **“SEC. 2215. DUTIES AND AUTHORITIES RELATING TO .GOV**
16 **INTERNET DOMAIN.”;**

17 (B) in the second section 2215 (6 U.S.C.
18 665b; relating to the joint cyber planning of-
19 fice), by amending the section enumerator and
20 heading to read as follows:

21 **“SEC. 2216. JOINT CYBER PLANNING OFFICE.”;**

22 (C) in the third section 2215 (6 U.S.C.
23 665c; relating to the Cybersecurity State Coor-
24 dinator), by amending the section enumerator
25 and heading to read as follows:

1 **“SEC. 2217. CYBERSECURITY STATE COORDINATOR.”;**

2 (D) in the fourth section 2215 (6 U.S.C.
3 665d; relating to Sector Risk Management
4 Agencies), by amending the section enumerator
5 and heading to read as follows:

6 **“SEC. 2218. SECTOR RISK MANAGEMENT AGENCIES.”;**

7 (E) in section 2216 (6 U.S.C. 665e; relat-
8 ing to the Cybersecurity Advisory Committee),
9 by amending the section enumerator and head-
10 ing to read as follows:

11 **“SEC. 2219. CYBERSECURITY ADVISORY COMMITTEE.”; and**

12 (F) in section 2217 (6 U.S.C. 665f; relat-
13 ing to Cybersecurity Education and Training
14 Programs), by amending the section enu-
15 merator and heading to read as follows:

16 **“SEC. 2220. CYBERSECURITY EDUCATION AND TRAINING
17 PROGRAMS.”.**

18 (2) CONSOLIDATED APPROPRIATIONS ACT,
19 2021.—Paragraph (1) of section 904(b) of division U
20 of the Consolidated Appropriations Act, 2021 (Pub-
21 lic Law 116–260) is amended, in the matter pre-
22 ceding subparagraph (A), by inserting “of 2002”
23 after “Homeland Security Act”.

24 (b) CLERICAL AMENDMENT.—The table of contents
25 in section 1(b) of the Homeland Security Act of 2002 is

1 amended by striking the items relating to sections 2214
2 through 2217 and inserting the following new items:

“Sec. 2214. National Asset Database.

“Sec. 2215. Duties and authorities relating to .gov internet domain.

“Sec. 2216. Joint cyber planning office.

“Sec. 2217. Cybersecurity State Coordinator.

“Sec. 2218. Sector Risk Management Agencies.

“Sec. 2219. Cybersecurity Advisory Committee.

“Sec. 2220. Cybersecurity Education and Training Programs.”.

3 **SEC. 5422. STATE AND LOCAL CYBERSECURITY GRANT PRO-**
4 **GRAM.**

5 (a) IN GENERAL.—Subtitle A of title XXII of the
6 Homeland Security Act of 2002 (6 U.S.C. 651 et seq.),
7 as amended by section 5321 of this Act, is further amend-
8 ed by adding at the end the following new sections:

9 **“SEC. 2220A. STATE AND LOCAL CYBERSECURITY GRANT**
10 **PROGRAM.**

11 “(a) DEFINITIONS.—In this section:

12 “(1) CYBER THREAT INDICATOR.—The term
13 ‘cyber threat indicator’ has the meaning given the
14 term in section 102 of the Cybersecurity Act of 2015
15 (6 U.S.C. 1501).

16 “(2) CYBERSECURITY PLAN.—The term ‘Cyber-
17 security Plan’ means a plan submitted by an eligible
18 entity under subsection (e)(1).

19 “(3) ELIGIBLE ENTITY.—The term ‘eligible en-
20 tity’ means—

21 “(A) a State; or

1 “(B) an Indian Tribe that, not later than
2 120 days after the date of the enactment of this
3 section or not later than 120 days before the
4 start of any fiscal year in which a grant under
5 this section is awarded—

6 “(i) notifies the Secretary that the In-
7 dian Tribe intends to develop a Cybersecu-
8 rity Plan; and

9 “(ii) agrees to forfeit any distribution
10 under subsection (n)(2).

11 “(4) INCIDENT.—The term ‘incident’ has the
12 meaning given the term in section 2209.

13 “(5) INDIAN TRIBE.—The term ‘Indian Tribe’
14 has the meaning given such term in section 4(e) of
15 the of the Indian Self-Determination and Education
16 Assistance Act (25 U.S.C. 5304(e)).

17 “(6) INFORMATION SHARING AND ANALYSIS OR-
18 GANIZATION.—The term ‘information sharing and
19 analysis organization’ has the meaning given the
20 term in section 2222.

21 “(7) INFORMATION SYSTEM.—The term ‘infor-
22 mation system’ has the meaning given the term in
23 section 102 of the Cybersecurity Act of 2015 (6
24 U.S.C. 1501).

1 “(8) ONLINE SERVICE.—The term ‘online serv-
2 ice’ means any internet-facing service, including a
3 website, email, virtual private network, or custom
4 application.

5 “(9) RANSOMWARE INCIDENT.—The term
6 ‘ransomware incident’ means an incident that actu-
7 ally or imminently jeopardizes, without lawful au-
8 thority, the integrity, confidentiality, or availability
9 of information on an information system, or actually
10 or imminently jeopardizes, without lawful authority,
11 an information system for the purpose of coercing
12 the information system’s owner, operator, or another
13 person.

14 “(10) STATE AND LOCAL CYBERSECURITY
15 GRANT PROGRAM.—The term ‘State and Local Cy-
16 bersecurity Grant Program’ means the program es-
17 tablished under subsection (b).

18 “(11) STATE AND LOCAL CYBERSECURITY RE-
19 SILIENCE COMMITTEE.—The term ‘State and Local
20 Cybersecurity Resilience Committee’ means the com-
21 mittee established under subsection (o)(1).

22 “(12) TRIBAL ORGANIZATION.—The term ‘Trib-
23 al organization’ has the meaning given such term in
24 section 4(l) of the of the Indian Self-Determination
25 and Education Assistance Act (25 U.S.C. 5304(l)).

1 “(b) ESTABLISHMENT.—

2 “(1) IN GENERAL.—The Secretary, acting
3 through the Director, shall establish a program, to
4 be known as the ‘the State and Local Cybersecurity
5 Grant Program’, to award grants to eligible entities
6 to address cybersecurity risks and cybersecurity
7 threats to information systems of State, local, or
8 Tribal organizations.

9 “(2) APPLICATION.—An eligible entity seeking
10 a grant under the State and Local Cybersecurity
11 Grant Program shall submit to the Secretary an ap-
12 plication at such time, in such manner, and con-
13 taining such information as the Secretary may re-
14 quire.

15 “(c) BASELINE REQUIREMENTS.—An eligible entity
16 or multistate group that receives a grant under this sec-
17 tion shall use the grant in compliance with—

18 “(1)(A) the Cybersecurity Plan of the eligible
19 entity or the Cybersecurity Plans of the eligible enti-
20 ties that comprise the multistate group; and

21 “(B) the Homeland Security Strategy to Im-
22 prove the Cybersecurity of State, Local, Tribal, and
23 Territorial Governments developed under section
24 2210(e)(1); or

1 “(2) activities carried out under paragraphs
2 (3), (4), and (5) of subsection (h).

3 “(d) ADMINISTRATION.—The State and Local Cyber-
4 security Grant Program shall be administered in the same
5 office of the Department that administers grants made
6 under sections 2003 and 2004.

7 “(e) CYBERSECURITY PLANS.—

8 “(1) IN GENERAL.—An eligible entity applying
9 for a grant under this section shall submit to the
10 Secretary a Cybersecurity Plan for approval.

11 “(2) REQUIRED ELEMENTS.—A Cybersecurity
12 Plan of an eligible entity shall—

13 “(A) incorporate, to the extent practicable,
14 any existing plans of the eligible entity to pro-
15 tect against cybersecurity risks and cybersecu-
16 rity threats to information systems of State,
17 local, or Tribal organizations;

18 “(B) describe, to the extent practicable,
19 how the eligible entity will—

20 “(i) manage, monitor, and track infor-
21 mation systems, applications, and user ac-
22 counts owned or operated by or on behalf
23 of the eligible entity or by local or Tribal
24 organizations within the jurisdiction of the
25 eligible entity and the information tech-

1 nology deployed on those information sys-
2 tems, including legacy information systems
3 and information technology that are no
4 longer supported by the manufacturer of
5 the systems or technology;

6 “(ii) monitor, audit, and track activity
7 between information systems, applications,
8 and user accounts owned or operated by or
9 on behalf of the eligible entity or by local
10 or Tribal organizations within the jurisdic-
11 tion of the eligible entity and between
12 those information systems and information
13 systems not owned or operated by the eligi-
14 ble entity or by local or Tribal organiza-
15 tions within the jurisdiction of the eligible
16 entity;

17 “(iii) enhance the preparation, re-
18 sponse, and resilience of information sys-
19 tems, applications, and user accounts
20 owned or operated by or on behalf of the
21 eligible entity or local or Tribal organiza-
22 tions against cybersecurity risks and cyber-
23 security threats;

24 “(iv) implement a process of contin-
25 uous cybersecurity vulnerability assess-

1 ments and threat mitigation practices
2 prioritized by degree of risk to address cy-
3 bersecurity risks and cybersecurity threats
4 on information systems of the eligible enti-
5 ty or local or Tribal organizations;

6 “(v) ensure that State, local, and
7 Tribal organizations that own or operate
8 information systems that are located with-
9 in the jurisdiction of the eligible entity—

10 “(I) adopt best practices and
11 methodologies to enhance cybersecu-
12 rity, such as the practices set forth in
13 the cybersecurity framework developed
14 by, and the cyber supply chain risk
15 management best practices identified
16 by, the National Institute of Stand-
17 ards and Technology; and

18 “(II) utilize knowledge bases of
19 adversary tools and tactics to assess
20 risk;

21 “(vi) promote the delivery of safe, rec-
22 ognizable, and trustworthy online services
23 by State, local, and Tribal organizations,
24 including through the use of the .gov inter-
25 net domain;

1 “(vii) ensure continuity of operations
2 of the eligible entity and local, and Tribal
3 organizations in the event of a cybersecu-
4 rity incident (including a ransomware inci-
5 dent), including by conducting exercises to
6 practice responding to such an incident;

7 “(viii) use the National Initiative for
8 Cybersecurity Education Cybersecurity
9 Workforce Framework developed by the
10 National Institute of Standards and Tech-
11 nology to identify and mitigate any gaps in
12 the cybersecurity workforces of State,
13 local, or Tribal organizations, enhance re-
14 cruitment and retention efforts for such
15 workforces, and bolster the knowledge,
16 skills, and abilities of State, local, and
17 Tribal organization personnel to address
18 cybersecurity risks and cybersecurity
19 threats, such as through cybersecurity hy-
20 giene training;

21 “(ix) ensure continuity of communica-
22 tions and data networks within the juris-
23 diction of the eligible entity between the el-
24 igible entity and local and Tribal organiza-
25 tions that own or operate information sys-

1 tems within the jurisdiction of the eligible
2 entity in the event of an incident involving
3 such communications or data networks
4 within the jurisdiction of the eligible entity;

5 “(x) assess and mitigate, to the great-
6 est degree possible, cybersecurity risks and
7 cybersecurity threats related to critical in-
8 frastructure and key resources, the deg-
9 radation of which may impact the perform-
10 ance of information systems within the ju-
11 risdiction of the eligible entity;

12 “(xi) enhance capabilities to share
13 cyber threat indicators and related infor-
14 mation between the eligible entity and local
15 and Tribal organizations that own or oper-
16 ate information systems within the juris-
17 diction of the eligible entity, including by
18 expanding existing information-sharing
19 agreements with the Department;

20 “(xii) enhance the capability of the el-
21 igible entity to share cyber threat indictors
22 and related information with the Depart-
23 ment;

24 “(xiii) leverage cybersecurity services
25 offered by the Department;

1 “(xiv) develop and coordinate strate-
2 gies to address cybersecurity risks and cy-
3 bersecurity threats to information systems
4 of the eligible entity in consultation with—
5 “(I) local and Tribal organiza-
6 tions within the jurisdiction of the eli-
7 gible entity; and
8 “(II) as applicable—
9 “(aa) States that neighbor
10 the jurisdiction of the eligible en-
11 tity or, as appropriate, members
12 of an information sharing and
13 analysis organization; and
14 “(bb) countries that neigh-
15 bor the jurisdiction of the eligible
16 entity; and
17 “(xv) implement an information tech-
18 nology and operational technology mod-
19 ernization cybersecurity review process
20 that ensures alignment between informa-
21 tion technology and operational technology
22 cybersecurity objectives;
23 “(C) describe, to the extent practicable, the
24 individual responsibilities of the eligible entity
25 and local and Tribal organizations within the

1 jurisdiction of the eligible entity in imple-
2 menting the plan;

3 “(D) outline, to the extent practicable, the
4 necessary resources and a timeline for imple-
5 menting the plan; and

6 “(E) describe how the eligible entity will
7 measure progress toward implementing the
8 plan.

9 “(3) DISCRETIONARY ELEMENTS.—A Cyberse-
10 curity Plan of an eligible entity may include a de-
11 scription of—

12 “(A) cooperative programs developed by
13 groups of local and Tribal organizations within
14 the jurisdiction of the eligible entity to address
15 cybersecurity risks and cybersecurity threats;
16 and

17 “(B) programs provided by the eligible en-
18 tity to support local and Tribal organizations
19 and owners and operators of critical infrastruc-
20 ture to address cybersecurity risks and cyberse-
21 curity threats.

22 “(4) MANAGEMENT OF FUNDS.—An eligible en-
23 tity applying for a grant under this section shall
24 agree to designate the Chief Information Officer, the
25 Chief Information Security Officer, or an equivalent

1 official of the eligible entity as the primary official
2 for the management and allocation of funds awarded
3 under this section.

4 “(f) MULTISTATE GRANTS.—

5 “(1) IN GENERAL.—The Secretary, acting
6 through the Director, may award grants under this
7 section to a group of two or more eligible entities to
8 support multistate efforts to address cybersecurity
9 risks and cybersecurity threats to information sys-
10 tems within the jurisdictions of the eligible entities.

11 “(2) SATISFACTION OF OTHER REQUIRE-
12 MENTS.—In order to be eligible for a multistate
13 grant under this subsection, each eligible entity that
14 comprises a multistate group shall submit to the
15 Secretary—

16 “(A) a Cybersecurity Plan for approval in
17 accordance with subsection (i); and

18 “(B) a plan for establishing a cybersecu-
19 rity planning committee under subsection (g).

20 “(3) APPLICATION.—

21 “(A) IN GENERAL.—A multistate group
22 applying for a multistate grant under para-
23 graph (1) shall submit to the Secretary an ap-
24 plication at such time, in such manner, and

1 containing such information as the Secretary
2 may require.

3 “(B) MULTISTATE PROJECT DESCRIPTION.—An application of a multistate group
4 under subparagraph (A) shall include a plan de-
5 scribing—
6

7 “(i) the division of responsibilities
8 among the eligible entities that comprise
9 the multistate group for administering the
10 grant for which application is being made;

11 “(ii) the distribution of funding from
12 such a grant among the eligible entities
13 that comprise the multistate group; and

14 “(iii) how the eligible entities that
15 comprise the multistate group will work to-
16 gether to implement the Cybersecurity
17 Plan of each of those eligible entities.

18 “(g) PLANNING COMMITTEES.—

19 “(1) IN GENERAL.—An eligible entity that re-
20 ceives a grant under this section shall establish a cy-
21 bersecurity planning committee to—

22 “(A) assist in the development, implemen-
23 tation, and revision of the Cybersecurity Plan of
24 the eligible entity;

1 “(B) approve the Cybersecurity Plan of the
2 eligible entity; and

3 “(C) assist in the determination of effective
4 funding priorities for a grant under this
5 section in accordance with subsection (h).

6 “(2) COMPOSITION.—A committee of an eligible
7 entity established under paragraph (1) shall—

8 “(A) be comprised of representatives from
9 the eligible entity and counties, cities, towns,
10 Tribes, and public educational and health institutions
11 within the jurisdiction of the eligible entity;
12 and

13 “(B) include, as appropriate, representatives
14 of rural, suburban, and high-population
15 jurisdictions.

16 “(3) CYBERSECURITY EXPERTISE.—Not less
17 than one-half of the representatives of a committee
18 established under paragraph (1) shall have professional
19 experience relating to cybersecurity or information
20 technology.

21 “(4) RULE OF CONSTRUCTION REGARDING EXISTING
22 PLANNING COMMITTEES.—Nothing in this
23 subsection may be construed to require an eligible
24 entity to establish a cybersecurity planning committee
25 if the eligible entity has established and uses

1 a multijurisdictional planning committee or commis-
2 sion that meets, or may be leveraged to meet, the re-
3 quirements of this subsection.

4 “(h) USE OF FUNDS.—An eligible entity that receives
5 a grant under this section shall use the grant to—

6 “(1) implement the Cybersecurity Plan of the
7 eligible entity;

8 “(2) develop or revise the Cybersecurity Plan of
9 the eligible entity; or

10 “(3) assist with activities that address immi-
11 nent cybersecurity risks or cybersecurity threats to
12 the information systems of the eligible entity or a
13 local or Tribal organization within the jurisdiction of
14 the eligible entity.

15 “(i) APPROVAL OF PLANS.—

16 “(1) APPROVAL AS CONDITION OF GRANT.—Be-
17 fore an eligible entity may receive a grant under this
18 section, the Secretary, acting through the Director,
19 shall review the Cybersecurity Plan, or any revisions
20 thereto, of the eligible entity and approve such plan,
21 or revised plan, if it satisfies the requirements speci-
22 fied in paragraph (2).

23 “(2) PLAN REQUIREMENTS.—In approving a
24 Cybersecurity Plan of an eligible entity under this

1 subsection, the Director shall ensure that the Cyber-
2 security Plan—

3 “(A) satisfies the requirements of sub-
4 section (e)(2);

5 “(B) upon the issuance of the Homeland
6 Security Strategy to Improve the Cybersecurity
7 of State, Local, Tribal, and Territorial Govern-
8 ments authorized pursuant to section 2210(e),
9 complies, as appropriate, with the goals and ob-
10 jectives of the strategy; and

11 “(C) has been approved by the cybersecu-
12 rity planning committee of the eligible entity es-
13 tablished under subsection (g).

14 “(3) APPROVAL OF REVISIONS.—The Secretary,
15 acting through the Director, may approve revisions
16 to a Cybersecurity Plan as the Director determines
17 appropriate.

18 “(4) EXCEPTION.—Notwithstanding subsection
19 (e) and paragraph (1) of this subsection, the Sec-
20 retary may award a grant under this section to an
21 eligible entity that does not submit a Cybersecurity
22 Plan to the Secretary if—

23 “(A) the eligible entity certifies to the Sec-
24 retary that—

1 “(i) the activities that will be sup-
2 ported by the grant are integral to the de-
3 velopment of the Cybersecurity Plan of the
4 eligible entity; and

5 “(ii) the eligible entity will submit by
6 September 30, 2023, to the Secretary, a
7 Cybersecurity Plan for review, and if ap-
8 propriate, approval; or

9 “(B) the eligible entity certifies to the Sec-
10 retary, and the Director confirms, that the eli-
11 gible entity will use funds from the grant to as-
12 sist with the activities described in subsection
13 (h)(3).

14 “(j) LIMITATIONS ON USES OF FUNDS.—

15 “(1) IN GENERAL.—An eligible entity that re-
16 ceives a grant under this section may not use the
17 grant—

18 “(A) to supplant State, local, or Tribal
19 funds;

20 “(B) for any recipient cost-sharing con-
21 tribution;

22 “(C) to pay a demand for ransom in an at-
23 tempt to—

24 “(i) regain access to information or
25 an information system of the eligible entity

1 or of a local or Tribal organization within
2 the jurisdiction of the eligible entity; or

3 “(ii) prevent the disclosure of infor-
4 mation that has been removed without au-
5 thorization from an information system of
6 the eligible entity or of a local or Tribal or-
7 ganization within the jurisdiction of the eli-
8 gible entity;

9 “(D) for recreational or social purposes; or

10 “(E) for any purpose that does not address
11 cybersecurity risks or cybersecurity threats on
12 information systems of the eligible entity or of
13 a local or Tribal organization within the juris-
14 diction of the eligible entity.

15 “(2) PENALTIES.—In addition to any other
16 remedy available, the Secretary may take such ac-
17 tions as are necessary to ensure that a recipient of
18 a grant under this section uses the grant for the
19 purposes for which the grant is awarded.

20 “(3) RULE OF CONSTRUCTION.—Nothing in
21 paragraph (1) may be construed to prohibit the use
22 of grant funds provided to a State, local, or Tribal
23 organization for otherwise permissible uses under
24 this section on the basis that a State, local, or Trib-

1 al organization has previously used State, local, or
2 Tribal funds to support the same or similar uses.

3 “(k) OPPORTUNITY TO AMEND APPLICATIONS.—In
4 considering applications for grants under this section, the
5 Secretary shall provide applicants with a reasonable op-
6 portunity to correct defects, if any, in such applications
7 before making final awards.

8 “(l) APPORTIONMENT.—For fiscal year 2022 and
9 each fiscal year thereafter, the Secretary shall apportion
10 amounts appropriated to carry out this section among
11 States as follows:

12 “(1) BASELINE AMOUNT.—The Secretary shall
13 first apportion 0.25 percent of such amounts to each
14 of American Samoa, the Commonwealth of the
15 Northern Mariana Islands, Guam, the United States
16 Virgin Islands, and 0.75 percent of such amounts to
17 each of the remaining States.

18 “(2) REMAINDER.—The Secretary shall appor-
19 tion the remainder of such amounts in the ratio
20 that—

21 “(A) the population of each eligible entity,
22 bears to

23 “(B) the population of all eligible entities.

24 “(3) MINIMUM ALLOCATION TO INDIAN
25 TRIBES.—

1 “(A) IN GENERAL.—In apportioning
2 amounts under this section, the Secretary shall
3 ensure that, for each fiscal year, directly eligible
4 Tribes collectively receive, from amounts appro-
5 priated under the State and Local Cybersecu-
6 rity Grant Program, not less than an amount
7 equal to three percent of the total amount ap-
8 propriated for grants under this section.

9 “(B) ALLOCATION.—Of the amount re-
10 served under subparagraph (A), funds shall be
11 allocated in a manner determined by the Sec-
12 retary in consultation with Indian Tribes.

13 “(C) EXCEPTION.—This paragraph shall
14 not apply in any fiscal year in which the Sec-
15 retary—

16 “(i) receives fewer than five applica-
17 tions from Indian Tribes; or

18 “(ii) does not approve at least two ap-
19 plications from Indian Tribes.

20 “(m) FEDERAL SHARE.—

21 “(1) IN GENERAL.—The Federal share of the
22 cost of an activity carried out using funds made
23 available with a grant under this section may not ex-
24 ceed—

1 “(A) in the case of a grant to an eligible
2 entity—

3 “(i) for fiscal year 2022, 90 percent;

4 “(ii) for fiscal year 2023, 80 percent;

5 “(iii) for fiscal year 2024, 70 percent;

6 “(iv) for fiscal year 2025, 60 percent;

7 and

8 “(v) for fiscal year 2026 and each
9 subsequent fiscal year, 50 percent; and

10 “(B) in the case of a grant to a multistate
11 group—

12 “(i) for fiscal year 2022, 95 percent;

13 “(ii) for fiscal year 2023, 85 percent;

14 “(iii) for fiscal year 2024, 75 percent;

15 “(iv) for fiscal year 2025, 65 percent;

16 and

17 “(v) for fiscal year 2026 and each
18 subsequent fiscal year, 55 percent.

19 “(2) WAIVER.—The Secretary may waive or
20 modify the requirements of paragraph (1) for an In-
21 dian Tribe if the Secretary determines such a waiver
22 is in the public interest.

23 “(n) RESPONSIBILITIES OF GRANTEES.—

24 “(1) CERTIFICATION.—Each eligible entity or
25 multistate group that receives a grant under this

1 section shall certify to the Secretary that the grant
2 will be used—

3 “(A) for the purpose for which the grant
4 is awarded; and

5 “(B) in compliance with, as the case may
6 be—

7 “(i) the Cybersecurity Plan of the eli-
8 gible entity;

9 “(ii) the Cybersecurity Plans of the eli-
10 gible entities that comprise the multistate
11 group; or

12 “(iii) a purpose approved by the Sec-
13 retary under subsection (h) or pursuant to
14 an exception under subsection (i).

15 “(2) AVAILABILITY OF FUNDS TO LOCAL AND
16 TRIBAL ORGANIZATIONS.—Not later than 45 days
17 after the date on which an eligible entity or
18 multistate group receives a grant under this section,
19 the eligible entity or multistate group shall, without
20 imposing unreasonable or unduly burdensome re-
21 quirements as a condition of receipt, obligate or oth-
22 erwise make available to local and Tribal organiza-
23 tions within the jurisdiction of the eligible entity or
24 the eligible entities that comprise the multistate
25 group, and as applicable, consistent with the Cyber-

1 security Plan of the eligible entity or the Cybersecu-
2 rity Plans of the eligible entities that comprise the
3 multistate group—

4 “(A) not less than 80 percent of funds
5 available under the grant;

6 “(B) with the consent of the local and
7 Tribal organizations, items, services, capabili-
8 ties, or activities having a value of not less than
9 80 percent of the amount of the grant; or

10 “(C) with the consent of the local and
11 Tribal organizations, grant funds combined
12 with other items, services, capabilities, or activi-
13 ties having the total value of not less than 80
14 percent of the amount of the grant.

15 “(3) CERTIFICATIONS REGARDING DISTRIBUTION OF GRANT FUNDS TO LOCAL AND TRIBAL ORGANIZATIONS.—An eligible entity or multistate group shall certify to the Secretary that the eligible entity or multistate group has made the distribution to local, Tribal, and territorial governments required under paragraph (2).

22 “(4) EXTENSION OF PERIOD.—

23 “(A) IN GENERAL.—An eligible entity or
24 multistate group may request in writing that
25 the Secretary extend the period of time speci-

1 fied in paragraph (2) for an additional period
2 of time.

3 “(B) APPROVAL.—The Secretary may ap-
4 prove a request for an extension under subpara-
5 graph (A) if the Secretary determines the ex-
6 tension is necessary to ensure that the obliga-
7 tion and expenditure of grant funds align with
8 the purpose of the State and Local Cybersecu-
9 rity Grant Program.

10 “(5) EXCEPTION.—Paragraph (2) shall not
11 apply to the District of Columbia, the Common-
12 wealth of Puerto Rico, American Samoa, the Com-
13 monwealth of the Northern Mariana Islands, Guam,
14 the United States Virgin Islands, or an Indian
15 Tribe.

16 “(6) DIRECT FUNDING.—If an eligible entity
17 does not make a distribution to a local or Tribal or-
18 ganization required in accordance with paragraph
19 (2), the local or Tribal organization may petition the
20 Secretary to request that grant funds be provided di-
21 rectly to the local or Tribal organization.

22 “(7) PENALTIES.—In addition to other rem-
23 edies available to the Secretary, the Secretary may
24 terminate or reduce the amount of a grant awarded
25 under this section to an eligible entity or distribute

1 grant funds previously awarded to such eligible enti-
2 ty directly to the appropriate local or Tribal organi-
3 zation as a replacement grant in an amount the Sec-
4 retary determines appropriate if such eligible entity
5 violates a requirement of this subsection.

6 “(o) ADVISORY COMMITTEE.—

7 “(1) ESTABLISHMENT.—Not later than 120
8 days after the date of enactment of this section, the
9 Director shall establish a State and Local Cyberse-
10 curity Resilience Committee to provide State, local,
11 and Tribal stakeholder expertise, situational aware-
12 ness, and recommendations to the Director, as ap-
13 propriate, regarding how to—

14 “(A) address cybersecurity risks and cyber-
15 security threats to information systems of
16 State, local, or Tribal organizations; and

17 “(B) improve the ability of State, local,
18 and Tribal organizations to prevent, protect
19 against, respond to, mitigate, and recover from
20 such cybersecurity risks and cybersecurity
21 threats.

22 “(2) DUTIES.—The committee established
23 under paragraph (1) shall—

1 “(A) submit to the Director recommenda-
2 tions that may inform guidance for applicants
3 for grants under this section;

4 “(B) upon the request of the Director, pro-
5 vide to the Director technical assistance to in-
6 form the review of Cybersecurity Plans sub-
7 mitted by applicants for grants under this sec-
8 tion, and, as appropriate, submit to the Direc-
9 tor recommendations to improve those plans
10 prior to the approval of the plans under sub-
11 section (i);

12 “(C) advise and provide to the Director
13 input regarding the Homeland Security Strat-
14 egy to Improve Cybersecurity for State, Local,
15 Tribal, and Territorial Governments required
16 under section 2210;

17 “(D) upon the request of the Director, pro-
18 vide to the Director recommendations, as ap-
19 propriate, regarding how to—

20 “(i) address cybersecurity risks and
21 cybersecurity threats on information sys-
22 tems of State, local, or Tribal organiza-
23 tions; and

1 “(ii) improve the cybersecurity resil-
2 ience of State, local, or Tribal organiza-
3 tions; and

4 “(E) regularly coordinate with the State,
5 Local, Tribal and Territorial Government Co-
6 ordinating Council, within the Critical Infra-
7 structure Partnership Advisory Council, estab-
8 lished under section 871.

9 “(3) MEMBERSHIP.—

10 “(A) NUMBER AND APPOINTMENT.—The
11 State and Local Cybersecurity Resilience Com-
12 mittee established pursuant to paragraph (1)
13 shall be composed of 15 members appointed by
14 the Director, as follows:

15 “(i) Two individuals recommended to
16 the Director by the National Governors As-
17 sociation.

18 “(ii) Two individuals recommended to
19 the Director by the National Association of
20 State Chief Information Officers.

21 “(iii) One individual recommended to
22 the Director by the National Guard Bu-
23 reau.

1 “(iv) Two individuals recommended to
2 the Director by the National Association of
3 Counties.

4 “(v) One individual recommended to
5 the Director by the National League of
6 Cities.

7 “(vi) One individual recommended to
8 the Director by the United States Con-
9 ference of Mayors.

10 “(vii) One individual recommended to
11 the Director by the Multi-State Informa-
12 tion Sharing and Analysis Center.

13 “(viii) One individual recommended to
14 the Director by the National Congress of
15 American Indians.

16 “(viii) Four individuals who have edu-
17 cational and professional experience relat-
18 ing to cybersecurity work or cybersecurity
19 policy.

20 “(B) TERMS.—

21 “(i) IN GENERAL.—Subject to clause
22 (ii), each member of the State and Local
23 Cybersecurity Resilience Committee shall
24 be appointed for a term of two years.

1 “(ii) REQUIREMENT.—At least two
2 members of the State and Local Cyberse-
3 curity Resilience Committee shall also be
4 members of the State, Local, Tribal and
5 Territorial Government Coordinating
6 Council, within the Critical Infrastructure
7 Partnership Advisory Council, established
8 under section 871.

9 “(iii) EXCEPTION.—A term of a mem-
10 ber of the State and Local Cybersecurity
11 Resilience Committee shall be three years
12 if the member is appointed initially to the
13 Committee upon the establishment of the
14 Committee.

15 “(iv) TERM REMAINDERS.—Any mem-
16 ber of the State and Local Cybersecurity
17 Resilience Committee appointed to fill a
18 vacancy occurring before the expiration of
19 the term for which the member’s prede-
20 cessor was appointed shall be appointed
21 only for the remainder of such term. A
22 member may serve after the expiration of
23 such member’s term until a successor has
24 taken office.

1 “(v) VACANCIES.—A vacancy in the
2 State and Local Cybersecurity Resilience
3 Committee shall be filled in the manner in
4 which the original appointment was made.

5 “(C) PAY.—Members of the State and
6 Local Cybersecurity Resilience Committee shall
7 serve without pay.

8 “(4) CHAIRPERSON; VICE CHAIRPERSON.—The
9 members of the State and Local Cybersecurity Resilience
10 Committee shall select a chairperson and vice
11 chairperson from among members of the committee.

12 “(5) PERMANENT AUTHORITY.—Notwith-
13 standing section 14 of the Federal Advisory Com-
14 mittee Act (5 U.S.C. App.), the State and Local Cy-
15 bersecurity Resilience Committee shall be a perma-
16 nent authority.

17 “(p) REPORTS.—

18 “(1) ANNUAL REPORTS BY GRANT RECIPI-
19 ENTS.—

20 “(A) IN GENERAL.—Not later than one
21 year after an eligible entity or multistate group
22 receives funds under this section, the eligible
23 entity or multistate group shall submit to the
24 Secretary a report on the progress of the eligi-
25 ble entity or multistate group in implementing

1 the Cybersecurity Plan of the eligible entity or
2 Cybersecurity Plans of the eligible entities that
3 comprise the multistate group, as the case may
4 be.

5 “(B) ABSENCE OF PLAN.—Not later than
6 180 days after an eligible entity that does not
7 have a Cybersecurity Plan receives funds under
8 this section for developing its Cybersecurity
9 Plan, the eligible entity shall submit to the Sec-
10 retary a report describing how the eligible enti-
11 ty obligated and expended grant funds during
12 the fiscal year to—

13 “(i) so develop such a Cybersecurity
14 Plan; or

15 “(ii) assist with the activities de-
16 scribed in subsection (h)(3).

17 “(2) ANNUAL REPORTS TO CONGRESS.—Not
18 less frequently than once per year, the Secretary,
19 acting through the Director, shall submit to Con-
20 gress a report on the use of grants awarded under
21 this section and any progress made toward the fol-
22 lowing:

23 “(A) Achieving the objectives set forth in
24 the Homeland Security Strategy to Improve the
25 Cybersecurity of State, Local, Tribal, and Ter-

1 ritorial Governments, upon the date on which
2 the strategy is issued under section 2210.

3 “(B) Developing, implementing, or revising
4 Cybersecurity Plans.

5 “(C) Reducing cybersecurity risks and cy-
6 bersecurity threats to information systems, ap-
7 plications, and user accounts owned or operated
8 by or on behalf of State, local, and Tribal orga-
9 nizations as a result of the award of such
10 grants.

11 “(q) AUTHORIZATION OF APPROPRIATIONS.—There
12 are authorized to be appropriated for grants under this
13 section—

14 “(1) for each of fiscal years 2022 through
15 2026, \$500,000,000; and

16 “(2) for each subsequent fiscal year, such sums
17 as may be necessary.

18 **“SEC. 2220B. CYBERSECURITY RESOURCE GUIDE DEVELOP-**
19 **MENT FOR STATE, LOCAL, TRIBAL, AND TER-**
20 **RITORIAL GOVERNMENT OFFICIALS.**

21 “The Secretary, acting through the Director, shall
22 develop, regularly update, and maintain a resource guide
23 for use by State, local, Tribal, and territorial government
24 officials, including law enforcement officers, to help such
25 officials identify, prepare for, detect, protect against, re-

1 spond to, and recover from cybersecurity risks (as such
2 term is defined in section 2209), cybersecurity threats,
3 and incidents (as such term is defined in section 2209).”.

4 (b) CLERICAL AMENDMENT.—The table of contents
5 in section 1(b) of the Homeland Security Act of 2002, as
6 amended by section 5413, is further amended by inserting
7 after the item relating to section 2220 the following new
8 items:

“Sec. 2220A. State and Local Cybersecurity Grant Program.

“Sec. 2220B. Cybersecurity resource guide development for State, local, Tribal,
and territorial government officials.”.

9 **SEC. 5423. STRATEGY.**

10 (a) HOMELAND SECURITY STRATEGY TO IMPROVE
11 THE CYBERSECURITY OF STATE, LOCAL, TRIBAL, AND
12 TERRITORIAL GOVERNMENTS.—Section 2210 of the
13 Homeland Security Act of 2002 (6 U.S.C. 660) is amend-
14 ed by adding at the end the following new subsection:

15 “(e) HOMELAND SECURITY STRATEGY TO IMPROVE
16 THE CYBERSECURITY OF STATE, LOCAL, TRIBAL, AND
17 TERRITORIAL GOVERNMENTS.—

18 “(1) IN GENERAL.—

19 “(A) REQUIREMENT.—Not later than one
20 year after the date of the enactment of this
21 subsection, the Secretary, acting through the
22 Director, shall, in coordination with the heads
23 of appropriate Federal agencies, State, local,
24 Tribal, and territorial governments, the State

1 and Local Cybersecurity Resilience Committee
2 established under section 2220A, and other
3 stakeholders, as appropriate, develop and make
4 publicly available a Homeland Security Strategy
5 to Improve the Cybersecurity of State, Local,
6 Tribal, and Territorial Governments.

7 “(B) RECOMMENDATIONS AND REQUIRE-
8 MENTS.—The strategy required under subpara-
9 graph (A) shall—

10 “(i) provide recommendations relating
11 to the ways in which the Federal Govern-
12 ment should support and promote the abil-
13 ity of State, local, Tribal, and territorial
14 governments to identify, mitigate against,
15 protect against, detect, respond to, and re-
16 cover from cybersecurity risks (as such
17 term is defined in section 2209), cyberse-
18 curity threats, and incidents (as such term
19 is defined in section 2209); and

20 “(ii) establish baseline requirements
21 for cybersecurity plans under this section
22 and principles with which such plans shall
23 align.

24 “(2) CONTENTS.—The strategy required under
25 paragraph (1) shall—

1 “(A) identify capability gaps in the ability
2 of State, local, Tribal, and territorial govern-
3 ments to identify, protect against, detect, re-
4 spond to, and recover from cybersecurity risks,
5 cybersecurity threats, incidents, and
6 ransomware incidents;

7 “(B) identify Federal resources and capa-
8 bilities that are available or could be made
9 available to State, local, Tribal, and territorial
10 governments to help those governments identify,
11 protect against, detect, respond to, and recover
12 from cybersecurity risks, cybersecurity threats,
13 incidents, and ransomware incidents;

14 “(C) identify and assess the limitations of
15 Federal resources and capabilities available to
16 State, local, Tribal, and territorial governments
17 to help those governments identify, protect
18 against, detect, respond to, and recover from
19 cybersecurity risks, cybersecurity threats, inci-
20 dents, and ransomware incidents and make rec-
21 ommendations to address such limitations;

22 “(D) identify opportunities to improve the
23 coordination of the Agency with Federal and
24 non-Federal entities, such as the Multi-State

1 Information Sharing and Analysis Center, to
2 improve—

3 “(i) incident exercises, information
4 sharing and incident notification proce-
5 dures;

6 “(ii) the ability for State, local, Trib-
7 al, and territorial governments to volun-
8 tarily adapt and implement guidance in
9 Federal binding operational directives; and

10 “(iii) opportunities to leverage Federal
11 schedules for cybersecurity investments
12 under section 502 of title 40, United
13 States Code;

14 “(E) recommend new initiatives the Fed-
15 eral Government should undertake to improve
16 the ability of State, local, Tribal, and territorial
17 governments to identify, protect against, detect,
18 respond to, and recover from cybersecurity
19 risks, cybersecurity threats, incidents, and
20 ransomware incidents;

21 “(F) set short-term and long-term goals
22 that will improve the ability of State, local,
23 Tribal, and territorial governments to identify,
24 protect against, detect, respond to, and recover

1 from cybersecurity risks, cybersecurity threats,
2 incidents, and ransomware incidents; and

3 “(G) set dates, including interim bench-
4 marks, as appropriate for State, local, Tribal,
5 and territorial governments to establish baseline
6 capabilities to identify, protect against, detect,
7 respond to, and recover from cybersecurity
8 risks, cybersecurity threats, incidents, and
9 ransomware incidents.

10 “(3) CONSIDERATIONS.—In developing the
11 strategy required under paragraph (1), the Director,
12 in coordination with the heads of appropriate Fed-
13 eral agencies, State, local, Tribal, and territorial
14 governments, the State and Local Cybersecurity Re-
15 siliency Committee established under section 2220A,
16 and other stakeholders, as appropriate, shall con-
17 sider—

18 “(A) lessons learned from incidents that
19 have affected State, local, Tribal, and territorial
20 governments, and exercises with Federal and
21 non-Federal entities;

22 “(B) the impact of incidents that have af-
23 fected State, local, Tribal, and territorial gov-
24 ernments, including the resulting costs to such
25 governments;

1 “(C) the information related to the interest
2 and ability of state and non-state threat actors
3 to compromise information systems (as such
4 term is defined in section 102 of the Cybersecu-
5 rity Act of 2015 (6 U.S.C. 1501)) owned or op-
6 erated by State, local, Tribal, and territorial
7 governments;

8 “(D) emerging cybersecurity risks and cy-
9 bersecurity threats to State, local, Tribal, and
10 territorial governments resulting from the de-
11 ployment of new technologies; and

12 “(E) recommendations made by the State
13 and Local Cybersecurity Resilience Committee
14 established under section 2220A.

15 “(4) EXEMPTION.—Chapter 35 of title 44,
16 United States Code (commonly known as the ‘Paper-
17 work Reduction Act’), shall not apply to any action
18 to implement this subsection.”.

19 (b) RESPONSIBILITIES OF THE DIRECTOR OF THE
20 CYBERSECURITY AND INFRASTRUCTURE SECURITY AGEN-
21 CY.—Section 2202 of the Homeland Security Act of 2002
22 (6 U.S.C. 652) is amended—

23 (1) by redesignating subsections (d) through (i)
24 as subsections (e) through (j), respectively; and

1 (2) by inserting after subsection (c) the fol-
2 lowing new subsection:

3 “(d) **ADDITIONAL RESPONSIBILITIES.**—In addition
4 to the responsibilities under subsection (c), the Director
5 shall—

6 “(1) develop program guidance, in consultation
7 with the State and Local Government Cybersecurity
8 Resilience Committee established under section
9 2220A, for the State and Local Cybersecurity Grant
10 Program under such section or any other homeland
11 security assistance administered by the Department
12 to improve cybersecurity;

13 “(2) review, in consultation with the State and
14 Local Cybersecurity Resilience Committee, all cyber-
15 security plans of State, local, Tribal, and territorial
16 governments developed pursuant to any homeland
17 security assistance administered by the Department
18 to improve cybersecurity;

19 “(3) provide expertise and technical assistance
20 to State, local, Tribal, and territorial government of-
21 ficials with respect to cybersecurity; and

22 “(4) provide education, training, and capacity
23 development to enhance the security and resilience
24 of cybersecurity and infrastructure security.”.

1 (c) FEASIBILITY STUDY.—Not later than 270 days
2 after the date of the enactment of this Act, the Director
3 of the Cybersecurity and Infrastructure Security of the
4 Department of Homeland Security shall conduct a study
5 to assess the feasibility of implementing a short-term rota-
6 tional program for the detail to the Agency of approved
7 State, local, Tribal, and territorial government employees
8 in cyber workforce positions.

9 **SEC. 5424. CYBERSECURITY VULNERABILITIES.**

10 Section 2209 of the Homeland Security Act of 2002
11 (6 U.S.C. 659) is amended—

12 (1) in subsection (a)—

13 (A) by redesignating paragraphs (4)
14 through (8) as paragraphs (5) through (9), re-
15 spectively; and

16 (B) by inserting after paragraph (3) the
17 following new paragraph:

18 “(4) the term ‘cybersecurity vulnerability’ has
19 the meaning given the term ‘security vulnerability’
20 in section 102 of the Cybersecurity Information
21 Sharing Act of 2015 (6 U.S.C. 1501);”.

22 (2) in subsection (c)—

23 (A) in paragraph (5)—

24 (i) in subparagraph (A), by striking
25 “and” after the semicolon at the end;

1 (ii) by redesignating subparagraph
2 (B) as subparagraph (C);

3 (iii) by inserting after subparagraph
4 (A) the following new subparagraph:

5 “(B) sharing mitigation protocols to counter cy-
6 bersecurity vulnerabilities pursuant to subsection
7 (n); and”;

8 (iv) in subparagraph (C), as so redesi-
9 gnated, by inserting “and mitigation pro-
10 tocols to counter cybersecurity
11 vulnerabilities in accordance with subpara-
12 graph (B)” before “with Federal”;

13 (B) in paragraph (7)(C), by striking
14 “sharing” and inserting “share”;

15 (C) in paragraph (9), by inserting “mitiga-
16 tion protocols to counter cybersecurity
17 vulnerabilities,” after “measures,”;

18 (3) in subsection (e)(1)(G), by striking the
19 semicolon after “and” at the end;

20 (4) by redesignating subsection (o) as sub-
21 section (p); and

22 (5) by inserting after subsection (n) following
23 new subsection:

24 “(o) PROTOCOLS TO COUNTER CERTAIN CYBERSE-
25 CURITY VULNERABILITIES.—The Director may, as appro-

1 p r i a t e , i d e n t i f y , d e v e l o p , a n d d i s s e m i n a t e a c t i o n a b l e p r o t o -
2 c o l s t o m i t i g a t e c y b e r s e c u r i t y v u l n e r a b i l i t i e s t o i n f o r m a -
3 t i o n s y s t e m s a n d i n d u s t r i a l c o n t r o l s y s t e m s , i n c l u d i n g i n
4 c i r c u m s t a n c e s i n w h i c h s u c h v u l n e r a b i l i t i e s e x i s t b e c a u s e
5 s o f t w a r e o r h a r d w a r e i s n o l o n g e r s u p p o r t e d b y a v e n -
6 d o r . ” .

7 **SEC. 5425. CAPABILITIES OF THE CYBERSECURITY AND IN-**
8 **FRASTRUCTURE SECURITY AGENCY TO IDEN-**
9 **TIFY THREATS TO INDUSTRIAL CONTROL**
10 **SYSTEMS.**

11 (a) IN GENERAL.—Section 2209 of the Homeland
12 Security Act of 2002 (6 U.S.C. 659) is amended—

13 (1) in subsection (e)(1)—

14 (A) in subparagraph (G), by striking
15 “and;” after the semicolon;

16 (B) in subparagraph (H), by inserting
17 “and” after the semicolon; and

18 (C) by adding at the end the following new
19 subparagraph:

20 “(I) activities of the Center address the se-
21 curity of both information technology and oper-
22 ational technology, including industrial control
23 systems;”; and

24 (2) by adding at the end the following new sub-
25 section:

1 “(p) INDUSTRIAL CONTROL SYSTEMS.—The Director
2 shall maintain capabilities to identify and address threats
3 and vulnerabilities to products and technologies intended
4 for use in the automated control of critical infrastructure
5 processes. In carrying out this subsection, the Director
6 shall—

7 “(1) lead Federal Government efforts, in con-
8 sultation with Sector Risk Management Agencies, as
9 appropriate, to identify and mitigate cybersecurity
10 threats to industrial control systems, including su-
11 pervisory control and data acquisition systems;

12 “(2) maintain threat hunting and incident re-
13 sponse capabilities to respond to industrial control
14 system cybersecurity risks and incidents;

15 “(3) provide cybersecurity technical assistance
16 to industry end-users, product manufacturers, Sector
17 Risk Management Agencies, other Federal agencies,
18 and other industrial control system stakeholders to
19 identify, evaluate, assess, and mitigate
20 vulnerabilities;

21 “(4) collect, coordinate, and provide vulner-
22 ability information to the industrial control systems
23 community by, as appropriate, working closely with
24 security researchers, industry end-users, product
25 manufacturers, Sector Risk Management Agencies,

1 other Federal agencies, and other industrial control
2 systems stakeholders; and

3 “(5) conduct such other efforts and assistance
4 as the Secretary determines appropriate.”.

5 (b) REPORT TO CONGRESS.—Not later than 180 days
6 after the date of the enactment of this Act and every six
7 months thereafter during the subsequent 4-year period,
8 the Director of the Cybersecurity and Infrastructure Secu-
9 rity Agency of the Department of Homeland Security shall
10 provide to the Committee on Homeland Security of the
11 House of Representatives and the Committee on Home-
12 land Security and Governmental Affairs of the Senate a
13 briefing on the industrial control systems capabilities of
14 the Agency under section 2209 of the Homeland Security
15 Act of 2002 (6 U.S.C. 659), as amended by subsection
16 (a).

17 (c) GAO REVIEW.—Not later than 2 years after the
18 date of the enactment of this Act, the Comptroller General
19 of the United States shall review implementation of the
20 requirements of subsections (e)(1)(I) and (p) of section
21 2209 of the Homeland Security Act of 2002 (6 U.S.C.
22 659), as amended by subsection (a), and submit to the
23 Committee on Homeland Security of the House of Rep-
24 resentatives and the Committee on Homeland Security
25 and Governmental Affairs of the Senate a report that in-

1 cludes findings and recommendations relating to such im-
2 plementation. Such report shall include information on the
3 following:

4 (1) Any interagency coordination challenges to
5 the ability of the Director of the Cybersecurity and
6 Infrastructure Agency of the Department of Home-
7 land Security to lead Federal efforts to identify and
8 mitigate cybersecurity threats to industrial control
9 systems pursuant to subsection (p)(1) of such sec-
10 tion.

11 (2) The degree to which the Agency has ade-
12 quate capacity, expertise, and resources to carry out
13 threat hunting and incident response capabilities to
14 mitigate cybersecurity threats to industrial control
15 systems pursuant to subsection (p)(2) of such sec-
16 tion, as well as additional resources that would be
17 needed to close any operational gaps in such capa-
18 bilities.

19 (3) The extent to which industrial control sys-
20 tem stakeholders sought cybersecurity technical as-
21 sistance from the Agency pursuant to subsection
22 (p)(3) of such section, and the utility and effective-
23 ness of such technical assistance.

24 (4) The degree to which the Agency works with
25 security researchers and other industrial control sys-

1 tems stakeholders, pursuant to subsection (p)(4) of
2 such section, to provide vulnerability information to
3 the industrial control systems community.

4 **SEC. 5426. REPORT ON CYBERSECURITY VULNERABILITIES.**

5 (a) REPORT.—Not later than 1 year after the date
6 of the enactment of this Act, the Director of the Cyberse-
7 curity and Infrastructure Security Agency of the Depart-
8 ment of Homeland Security shall submit to the Committee
9 on Homeland Security of the House of Representatives
10 and the Committee on Homeland Security and Govern-
11 mental Affairs of the Senate a report on how the Agency
12 carries out subsection (n) of section 2209 of the Homeland
13 Security Act of 2002 to coordinate vulnerability disclo-
14 sures, including disclosures of cybersecurity vulnerabilities
15 (as such term is defined in such section), and subsection
16 (o) of such section (as added by section 5324) to dissemi-
17 nate actionable protocols to mitigate cybersecurity
18 vulnerabilities to information systems and industrial con-
19 trol systems, that include the following:

20 (1) A description of the policies and procedures
21 relating to the coordination of vulnerability disclo-
22 sures.

23 (2) A description of the levels of activity in fur-
24 therance of such subsections (n) and (o) of such sec-
25 tion 2209.

1 (3) Any plans to make further improvements to
2 how information provided pursuant to such sub-
3 sections can be shared (as such term is defined in
4 such section 2209) between the Department and in-
5 dustry and other stakeholders.

6 (4) Any available information on the degree to
7 which such information was acted upon by industry
8 and other stakeholders.

9 (5) A description of how privacy and civil lib-
10 erties are preserved in the collection, retention, use,
11 and sharing of vulnerability disclosures.

12 (b) FORM.—The report required under subsection (b)
13 shall be submitted in unclassified form but may contain
14 a classified annex.

15 **SEC. 5427. COMPETITION RELATING TO CYBERSECURITY**

16 **VULNERABILITIES.**

17 The Under Secretary for Science and Technology of
18 the Department of Homeland Security, in consultation
19 with the Director of the Cybersecurity and Infrastructure
20 Security Agency of the Department, may establish an in-
21 centive-based program that allows industry, individuals,
22 academia, and others to compete in identifying remedi-
23 ation solutions for cybersecurity vulnerabilities (as such
24 term is defined in section 2209 of the Homeland Security
25 Act of 2002, as amended by section 5325) to information

1 systems (as such term is defined in such section 2209)
2 and industrial control systems, including supervisory con-
3 trol and data acquisition systems.

4 **SEC. 5428. NATIONAL CYBER EXERCISE PROGRAM.**

5 (a) IN GENERAL.—Subtitle A of title XXII of the
6 Homeland Security Act of 2002 (6 U.S.C. 651 et seq.),
7 as amended by section 5322 of this Act, is further amend-
8 ed by adding at the end the following new section:

9 **“SEC. 2220C. NATIONAL CYBER EXERCISE PROGRAM.**

10 “(a) ESTABLISHMENT OF PROGRAM.—

11 “(1) IN GENERAL.—There is established in the
12 Agency the National Cyber Exercise Program (re-
13 ferred to in this section as the ‘Exercise Program’)
14 to evaluate the National Cyber Incident Response
15 Plan, and other related plans and strategies.

16 “(2) REQUIREMENTS.—

17 “(A) IN GENERAL.—The Exercise Program
18 shall be—

19 “(i) based on current risk assess-
20 ments, including credible threats,
21 vulnerabilities, and consequences;

22 “(ii) designed, to the extent prac-
23 ticable, to simulate the partial or complete
24 incapacitation of a government or critical

1 infrastructure network resulting from a
2 cyber incident;

3 “(iii) designed to provide for the sys-
4 tematic evaluation of cyber readiness and
5 enhance operational understanding of the
6 cyber incident response system and rel-
7 evant information-sharing agreements; and

8 “(iv) designed to promptly develop
9 after-action reports and plans that can
10 quickly incorporate lessons learned into fu-
11 ture operations.

12 “(B) MODEL EXERCISE SELECTION.—The
13 Exercise Program shall—

14 “(i) include a selection of model exer-
15 cises that government and private entities
16 can readily adapt for use; and

17 “(ii) aid such governments and pri-
18 vate entities with the design, implementa-
19 tion, and evaluation of exercises that—

20 “(I) conform to the requirements
21 described in subparagraph (A);

22 “(II) are consistent with any ap-
23 plicable national, State, local, or Trib-
24 al strategy or plan; and

1 “(III) provide for systematic
2 evaluation of readiness.

3 “(3) CONSULTATION.—In carrying out the Ex-
4 ercise Program, the Director may consult with ap-
5 propriate representatives from Sector Risk Manage-
6 ment Agencies, cybersecurity research stakeholders,
7 and Sector Coordinating Councils.

8 “(b) DEFINITIONS.—In this section:

9 “(1) STATE.—The term ‘State’ means any
10 State of the United States, the District of Columbia,
11 the Commonwealth of Puerto Rico, the Northern
12 Mariana Islands, the United States Virgin Islands,
13 Guam, American Samoa, and any other territory or
14 possession of the United States.

15 “(2) PRIVATE ENTITY.—The term ‘private enti-
16 ty’ has the meaning given such term in section 102
17 of the Cybersecurity Information Sharing Act of
18 2015 (6 U.S.C. 1501).”.

19 (b) CLERICAL AMENDMENT.—The table of contents
20 in section 1(b) of the Homeland Security Act of 2002, as
21 amended by section 5422 of this Act, is further amended
22 by adding after the item relating to section 2220B the
23 following new item:

 “Sec. 2220C. National Cyber Exercise Program.”.

1 **Subtitle C—Transportation**
2 **Security**

3 **SEC. 5431. SURVEY OF THE TRANSPORTATION SECURITY**
4 **ADMINISTRATION WORKFORCE REGARDING**
5 **COVID-19 RESPONSE.**

6 (a) SURVEY.—Not later than 1 year after the date
7 of the enactment of this Act, the Administrator of the
8 Transportation Security Administration (referred to in
9 this section as the “Administrator”), in consultation with
10 the labor organization certified as the exclusive represent-
11 ative of full- and part-time nonsupervisory Administration
12 personnel carrying out screening functions under section
13 44901 of title 49, United States Code, shall conduct a sur-
14 vey of the Transportation Security Administration (re-
15 ferred to in this section as the “Administration”) work-
16 force regarding the Administration’s response to the
17 COVID-19 pandemic. Such survey shall be conducted in
18 a manner that allows for the greatest practicable level of
19 workforce participation.

20 (b) CONTENTS.—In conducting the survey required
21 under subsection (a), the Administrator shall solicit feed-
22 back on the following:

23 (1) The Administration’s communication and
24 collaboration with the Administration’s workforce re-
25 garding the Administration’s response to the

1 COVID–19 pandemic and efforts to mitigate and
2 monitor transmission of COVID–19 among its work-
3 force, including through—

4 (A) providing employees with personal pro-
5 tective equipment and mandating its use;

6 (B) modifying screening procedures and
7 Administration operations to reduce trans-
8 mission among officers and passengers and en-
9 suring compliance with such changes;

10 (C) adjusting policies regarding scheduling,
11 leave, and telework;

12 (D) outreach as a part of contact tracing
13 when an employee has tested positive for
14 COVID–19; and

15 (E) encouraging COVID–19 vaccinations
16 and efforts to assist employees that seek to be
17 vaccinated such as communicating the avail-
18 ability of duty time for travel to vaccination
19 sites and recovery from vaccine side effects.

20 (2) Any other topic determined appropriate by
21 the Administrator.

22 (c) REPORT.—Not later than 30 days after com-
23 pleting the survey required under subsection (a), the Ad-
24 ministration shall provide a report summarizing the re-
25 sults of the survey to the Committee on Homeland Secu-

1 rity of the House of Representatives and the Committee
2 on Commerce, Science, and Transportation of the Senate.

3 **SEC. 5432. TRANSPORTATION SECURITY PREPAREDNESS**

4 **PLAN.**

5 (a) **PLAN REQUIRED.**—Section 114 of title 49,
6 United States Code, is amended by adding at the end the
7 following new subsection:

8 “(x) **TRANSPORTATION SECURITY PREPAREDNESS**
9 **PLAN.**—

10 “(1) **IN GENERAL.**—Not later than two years
11 after the date of the enactment of this subsection,
12 the Secretary of Homeland Security, acting through
13 the Administrator, in coordination with the Chief
14 Medical Officer of the Department of Homeland Se-
15 curity and in consultation with the partners identi-
16 fied under paragraphs (3)(A)(i) through (3)(A)(iv),
17 shall develop a transportation security preparedness
18 plan to address the event of a communicable disease
19 outbreak. The Secretary, acting through the Admin-
20 istrator, shall ensure such plan aligns with relevant
21 Federal plans and strategies for communicable dis-
22 ease outbreaks.

23 “(2) **CONSIDERATIONS.**—In developing the plan
24 required under paragraph (1), the Secretary, acting

1 through the Administrator, shall consider each of
2 the following:

3 “(A) The findings of the survey required
4 under section 5331 of the National Defense Au-
5 thorization Act for Fiscal Year 2022.

6 “(B) All relevant reports and recommenda-
7 tions regarding the Administration’s response
8 to the COVID–19 pandemic, including any re-
9 ports and recommendations issued by the
10 Comptroller General and the Inspector General
11 of the Department of Homeland Security.

12 “(C) Lessons learned from Federal inter-
13 agency efforts during the COVID–19 pandemic.

14 “(3) CONTENTS OF PLAN.—The plan developed
15 under paragraph (1) shall include each of the fol-
16 lowing:

17 “(A) Plans for communicating and collabo-
18 rating in the event of a communicable disease
19 outbreak with the following partners:

20 “(i) Appropriate Federal departments
21 and agencies, including the Department of
22 Health and Human Services, the Centers
23 for Disease Control and Prevention, the
24 Department of Transportation, the De-

1 partment of Labor, and appropriate inter-
2 agency task forces.

3 “(ii) The workforce of the Administra-
4 tion, including through the labor organiza-
5 tion certified as the exclusive representa-
6 tive of full- and part-time non-supervisory
7 Administration personnel carrying out
8 screening functions under section 44901 of
9 this title.

10 “(iii) International partners, including
11 the International Civil Aviation Organiza-
12 tion and foreign governments, airports,
13 and air carriers.

14 “(iv) Public and private stakeholders,
15 as such term is defined under subsection
16 (t)(1)(C).

17 “(v) The traveling public.

18 “(B) Plans for protecting the safety of the
19 Transportation Security Administration work-
20 force, including—

21 “(i) reducing the risk of commu-
22 nicable disease transmission at screening
23 checkpoints and within the Administra-
24 tion’s workforce related to the Administra-

1 tion’s transportation security operations
2 and mission;

3 “(ii) ensuring the safety and hygiene
4 of screening checkpoints and other
5 workstations;

6 “(iii) supporting equitable and appro-
7 priate access to relevant vaccines, prescrip-
8 tions, and other medical care; and

9 “(iv) tracking rates of employee ill-
10 ness, recovery, and death.

11 “(C) Criteria for determining the condi-
12 tions that may warrant the integration of addi-
13 tional actions in the aviation screening system
14 in response to the communicable disease out-
15 break and a range of potential roles and re-
16 sponsibilities that align with such conditions.

17 “(D) Contingency plans for temporarily
18 adjusting checkpoint operations to provide for
19 passenger and employee safety while maintain-
20 ing security during the communicable disease
21 outbreak.

22 “(E) Provisions setting forth criteria for
23 establishing an interagency task force or other
24 standing engagement platform with other ap-
25 propriate Federal departments and agencies, in-

1 including the Department of Health and Human
2 Services and the Department of Transportation,
3 to address such communicable disease outbreak.

4 “(F) A description of scenarios in which
5 the Administrator should consider exercising
6 authorities provided under subsection (g) and
7 for what purposes.

8 “(G) Considerations for assessing the ap-
9 propriateness of issuing security directives and
10 emergency amendments to regulated parties in
11 various modes of transportation, including sur-
12 face transportation, and plans for ensuring
13 compliance with such measures.

14 “(H) A description of any potential obsta-
15 cles, including funding constraints and limita-
16 tions to authorities, that could restrict the abil-
17 ity of the Administration to respond appro-
18 priately to a communicable disease outbreak.

19 “(4) DISSEMINATION.—Upon development of
20 the plan required under paragraph (1), the Adminis-
21 trator shall disseminate the plan to the partners
22 identified under paragraph (3)(A) and to the Com-
23 mittee on Homeland Security of the House of Rep-
24 resentatives and the Committee on Commerce,
25 Science, and Transportation of the Senate.

1 “(5) REVIEW OF PLAN.—Not later than two
2 years after the date on which the plan is dissemi-
3 nated under paragraph (4), and biennially there-
4 after, the Secretary, acting through the Adminis-
5 trator and in coordination with the Chief Medical
6 Officer of the Department of Homeland Security,
7 shall review the plan and, after consultation with the
8 partners identified under paragraphs (3)(A)(i)
9 through (3)(A)(iv), update the plan as appropriate.”.

10 (b) COMPTROLLER GENERAL REPORT.—Not later
11 than 1 year after the date on which the transportation
12 security preparedness plan required under subsection (x)
13 of section 114 of title 49, United States Code, as added
14 by subsection (a), is disseminated under paragraph (4) of
15 such subsection (x), the Comptroller General of the United
16 States shall submit to the Committee on Homeland Secu-
17 rity of the House of Representatives and the Committee
18 on Commerce, Science, and Transportation of the Senate
19 a report containing the results of a study assessing the
20 transportation security preparedness plan, including an
21 analysis of—

22 (1) whether such plan aligns with relevant Fed-
23 eral plans and strategies for communicable disease
24 outbreaks; and

1 (2) the extent to which the Transportation Se-
2 curity Administration is prepared to implement the
3 plan.

4 **SEC. 5433. AUTHORIZATION OF TRANSPORTATION SECU-**
5 **RITY ADMINISTRATION PERSONNEL DETAILS.**

6 (a) COORDINATION.—Pursuant to sections 106(m)
7 and 114(m) of title 49, United States Code, the Adminis-
8 trator of the Transportation Security Administration may
9 provide Transportation Security Administration per-
10 sonnel, who are not engaged in front line transportation
11 security efforts, to other components of the Department
12 and other Federal agencies to improve coordination with
13 such components and agencies to prepare for, protect
14 against, and respond to public health threats to the trans-
15 portation security system of the United States.

16 (b) BRIEFING.—Not later than 180 days after the
17 date of the enactment of this Act, the Administrator shall
18 brief the appropriate congressional committees regarding
19 efforts to improve coordination with other components of
20 the Department of Homeland Security and other Federal
21 agencies to prepare for, protect against, and respond to
22 public health threats to the transportation security system
23 of the United States.

1 **SEC. 5434. TRANSPORTATION SECURITY ADMINISTRATION**

2 **PREPAREDNESS.**

3 (a) ANALYSIS.—

4 (1) IN GENERAL.—The Administrator of the
5 Transportation Security Administration shall con-
6 duct an analysis of preparedness of the transpor-
7 tation security system of the United States for pub-
8 lic health threats. Such analysis shall assess, at a
9 minimum, the following:

10 (A) The risks of public health threats to
11 the transportation security system of the
12 United States, including to transportation hubs,
13 transportation security stakeholders, Transpor-
14 tation Security Administration (TSA) per-
15 sonnel, and passengers.

16 (B) Information sharing challenges among
17 relevant components of the Department, other
18 Federal agencies, international entities, and
19 transportation security stakeholders.

20 (C) Impacts to TSA policies and proce-
21 dures for securing the transportation security
22 system.

23 (2) COORDINATION.—The analysis conducted of
24 the risks described in paragraph (1)(A) shall be con-
25 ducted in coordination with the Chief Medical Offi-
26 cer of the Department of Homeland Security, the

1 Secretary of Health and Human Services, and trans-
2 portation security stakeholders.

3 (b) BRIEFING.—Not later than 180 days after the
4 date of the enactment of this Act, the Administrator shall
5 brief the appropriate congressional committees on the fol-
6 lowing:

7 (1) The analysis required under subsection (a).

8 (2) Technologies necessary to combat public
9 health threats at security screening checkpoints to
10 better protect from future public health threats TSA
11 personnel, passengers, aviation workers, and other
12 personnel authorized to access the sterile area of an
13 airport through such checkpoints, and the estimated
14 cost of technology investments needed to fully imple-
15 ment across the aviation system solutions to such
16 threats.

17 (3) Policies and procedures implemented by
18 TSA and transportation security stakeholders to
19 protect from public health threats TSA personnel,
20 passengers, aviation workers, and other personnel
21 authorized to access the sterile area through the se-
22 curity screening checkpoints, as well as future plans
23 for additional measures relating to such protection.

24 (4) The role of TSA in establishing priorities,
25 developing solutions, and coordinating and sharing

1 information with relevant domestic and international
2 entities during a public health threat to the trans-
3 portation security system, and how TSA can im-
4 prove its leadership role in such areas.

5 (c) DEFINITIONS.—In this section:

6 (1) The term “appropriate congressional com-
7 mittees” means—

8 (A) the Committee on Homeland Security
9 of the House of Representatives; and

10 (B) the Committee on Homeland Security
11 and Governmental Affairs and the Committee
12 on Commerce, Science, and Transportation of
13 the Senate.

14 (2) The term “sterile area” has the meaning
15 given such term in section 1540.5 of title 49, Code
16 of Federal Regulations.

17 (3) The term “TSA” means the Transportation
18 Security Administration.

19 **SEC. 5435. PLAN TO REDUCE THE SPREAD OF**
20 **CORONAVIRUS AT PASSENGER SCREENING**
21 **CHECKPOINTS.**

22 (a) IN GENERAL.—Not later than 90 days after the
23 date of the enactment of this Act, the Administrator, in
24 coordination with the Chief Medical Officer of the Depart-
25 ment of Homeland Security, and in consultation with the

1 Secretary of Health and Human Services and the Director
2 of the Centers for Disease Control and Prevention, shall
3 issue and commence implementing a plan to enhance, as
4 appropriate, security operations at airports during the
5 COVID–19 national emergency in order to reduce risk of
6 the spread of the coronavirus at passenger screening
7 checkpoints and among the TSA workforce.

8 (b) CONTENTS.—The plan required under subsection
9 (a) shall include the following:

10 (1) An identification of best practices developed
11 in response to the coronavirus among foreign gov-
12 ernments, airports, and air carriers conducting avia-
13 tion security screening operations, as well as among
14 Federal agencies conducting similar security screen-
15 ing operations outside of airports, including in loca-
16 tions where the spread of the coronavirus has been
17 successfully contained, that could be further inte-
18 grated into the United States aviation security sys-
19 tem.

20 (2) Specific operational changes to aviation se-
21 curity screening operations informed by the identi-
22 fication of best practices under paragraph (1) that
23 could be implemented without degrading aviation se-
24 curity and a corresponding timeline and costs for
25 implementing such changes.

1 (c) CONSIDERATIONS.—In carrying out the identi-
2 fication of best practices under subsection (b), the Admin-
3 istrator shall take into consideration the following:

4 (1) Aviation security screening procedures and
5 practices in place at security screening locations, in-
6 cluding procedures and practices implemented in re-
7 sponse to the coronavirus.

8 (2) Volume and average wait times at each such
9 security screening location.

10 (3) Public health measures already in place at
11 each such security screening location.

12 (4) The feasibility and effectiveness of imple-
13 menting similar procedures and practices in loca-
14 tions where such are not already in place.

15 (5) The feasibility and potential benefits to se-
16 curity, public health, and travel facilitation of con-
17 tinuing any procedures and practices implemented in
18 response to the COVID–19 national emergency be-
19 yond the end of such emergency.

20 (d) CONSULTATION.—In developing the plan required
21 under subsection (a), the Administrator may consult with
22 public and private stakeholders and the TSA workforce,
23 including through the labor organization certified as the
24 exclusive representative of full- and part-time non-

1 supervisory TSA personnel carrying out screening func-
2 tions under section 44901 of title 49, United States Code.

3 (e) SUBMISSION.—Upon issuance of the plan re-
4 quired under subsection (a), the Administrator shall sub-
5 mit the plan to the Committee on Homeland Security of
6 the House of Representatives and the Committee on Com-
7 merce, Science, and Transportation of the Senate.

8 (f) ISSUANCE AND IMPLEMENTATION.—The Admin-
9 istrator shall not be required to issue or implement, as
10 the case may be, the plan required under subsection (a)
11 upon the termination of the COVID–19 national emer-
12 gency except to the extent the Administrator determines
13 such issuance or implementation, as the case may be, to
14 be feasible and beneficial to security screening operations.

15 (g) GAO REVIEW.—Not later than 1 year after the
16 issuance of the plan required under subsection (a) (if such
17 plan is issued in accordance with subsection (f)), the
18 Comptroller General of the United States shall submit to
19 the Committee on Homeland Security of the House of
20 Representatives and the Committee on Commerce,
21 Science, and Transportation of the Senate a review, if ap-
22 propriate, of such plan and any efforts to implement such
23 plan.

24 (h) DEFINITIONS.—In this section:

1 (1) The term “Administrator” means the Ad-
2 ministrator of the Transportation Security Adminis-
3 tration.

4 (2) The term “coronavirus” has the meaning
5 given such term in section 506 of the Coronavirus
6 Preparedness and Response Supplemental Appro-
7 priations Act, 2020 (Public Law 116–123).

8 (3) The term “COVID–19 national emergency”
9 means the national emergency declared by the Presi-
10 dent under the National Emergencies Act (50
11 U.S.C. 1601 et seq.) on March 13, 2020, with re-
12 spect to the coronavirus.

13 (4) The term “public and private stakeholders”
14 has the meaning given such term in section
15 114(t)(1)(C) of title 49, United States Code.

16 (5) The term “TSA” means the Transportation
17 Security Administration.

18 **SEC. 5436. COMPTROLLER GENERAL REVIEW OF DEPART-**
19 **MENT OF HOMELAND SECURITY TRUSTED**
20 **TRAVELER PROGRAMS.**

21 Not later than one year after the date of the enact-
22 ment of this Act, the Comptroller General of the United
23 States shall conduct a review of Department of Homeland
24 Security trusted traveler programs. Such review shall ex-
25 amine the following:

1 (1) The extent to which the Department of
2 Homeland Security tracks data and monitors trends
3 related to trusted traveler programs, including root
4 causes for identity-matching errors resulting in an
5 individual's enrollment in a trusted traveler program
6 being reinstated.

7 (2) Whether the Department coordinates with
8 the heads of other relevant Federal, State, local,
9 Tribal, or territorial entities regarding redress proce-
10 dures for disqualifying offenses not covered by the
11 Department's own redress processes but which of-
12 fenses impact an individual's enrollment in a trusted
13 traveler program.

14 (3) How the Department may improve individ-
15 uals' access to reconsideration procedures regarding
16 a disqualifying offense for enrollment in a trusted
17 traveler program that requires the involvement of
18 any other Federal, State, local, Tribal, or territorial
19 entity.

20 (4) The extent to which travelers are informed
21 about reconsideration procedures regarding enroll-
22 ment in a trusted traveler program.

1 **SEC. 5437. ENROLLMENT REDRESS WITH RESPECT TO DE-**
2 **PARTMENT OF HOMELAND SECURITY TRUST-**
3 **ED TRAVELER PROGRAMS.**

4 Notwithstanding any other provision of law, the Sec-
5 retary of Homeland Security shall, with respect to an indi-
6 vidual whose enrollment in a trusted traveler program was
7 revoked in error extend by an amount of time equal to
8 the period of revocation the period of active enrollment
9 in such a program upon reenrollment in such a program
10 by such an individual.

11 **SEC. 5438. THREAT INFORMATION SHARING.**

12 (a) **PRIORITIZATION.**—The Secretary of Homeland
13 Security shall prioritize the assignment of officers and in-
14 telligence analysts under section 210A of the Homeland
15 Security Act of 2002 (6 U.S.C. 124h) from the Transpor-
16 tation Security Administration and, as appropriate, from
17 the Office of Intelligence and Analysis of the Department
18 of Homeland Security, to locations with participating
19 State, local, and regional fusion centers in jurisdictions
20 with a high-risk surface transportation asset in order to
21 enhance the security of such assets, including by improv-
22 ing timely sharing, in a manner consistent with the protec-
23 tion of privacy rights, civil rights, and civil liberties, of
24 information regarding threats of terrorism and other
25 threats, including targeted violence.

1 (b) INTELLIGENCE PRODUCTS.—Officers and intel-
2 ligence analysts assigned to locations with participating
3 State, local, and regional fusion centers under this section
4 shall participate in the generation and dissemination of
5 transportation security intelligence products, with an em-
6 phasis on such products that relate to threats of terrorism
7 and other threats, including targeted violence, to surface
8 transportation assets that—

9 (1) assist State, local, and Tribal law enforce-
10 ment agencies in deploying their resources, including
11 personnel, most efficiently to help detect, prevent,
12 investigate, apprehend, and respond to such threats;

13 (2) promote more consistent and timely sharing
14 with and among jurisdictions of threat information;
15 and

16 (3) enhance the Department of Homeland Secu-
17 rity's situational awareness of such threats.

18 (c) CLEARANCES.—The Secretary of Homeland Secu-
19 rity shall make available to appropriate owners and opera-
20 tors of surface transportation assets, and to any other per-
21 son that the Secretary determines appropriate to foster
22 greater sharing of classified information relating to
23 threats of terrorism and other threats, including targeted
24 violence, to surface transportation assets, the process of
25 application for security clearances under Executive Order

1 No. 13549 (75 Fed. Reg. 162; relating to a classified na-
2 tional security information program) or any successor Ex-
3 ecutive order.

4 (d) GAO REPORT.—Not later than 2 years after the
5 date of the enactment of this Act, the Comptroller General
6 of the United States shall submit to the Committee on
7 Homeland Security of the House of Representatives and
8 the Committee on Homeland Security and Governmental
9 Affairs of the Senate a review of the implementation of
10 this section, together with any recommendations to im-
11 prove information sharing with State, local, Tribal, terri-
12 torial, and private sector entities to prevent, identify, and
13 respond to threats of terrorism and other threats, includ-
14 ing targeted violence, to surface transportation assets.

15 (e) DEFINITIONS.—In this section:

16 (1) The term “surface transportation asset” in-
17 cludes facilities, equipment, or systems used to pro-
18 vide transportation services by—

19 (A) a public transportation agency (as
20 such term is defined in section 1402(5) of the
21 Implementing Recommendations of the 9/11
22 Commission Act of 2007 (Public Law 110–53;
23 6 U.S.C. 1131(5)));

1 (B) a railroad carrier (as such term is de-
2 fined in section 20102(3) of title 49, United
3 States Code);

4 (C) an owner or operator of—

5 (i) an entity offering scheduled, fixed-
6 route transportation services by over-the-
7 road bus (as such term is defined in sec-
8 tion 1501(4) of the Implementing Rec-
9 ommendations of the 9/11 Commission Act
10 of 2007 (Public Law 110–53; 6 U.S.C.
11 1151(4))); or

12 (ii) a bus terminal; or

13 (D) other transportation facilities, equip-
14 ment, or systems, as determined by the Sec-
15 retary.

16 (2) The term “targeted violence” means an in-
17 cident of violence in which an attacker selected a
18 particular target in order to inflict mass injury or
19 death with no discernable political or ideological mo-
20 tivation beyond mass injury or death.

21 (3) The term “terrorism” means the terms—

22 (A) domestic terrorism (as such term is de-
23 fined in section 2331(5) of title 18, United
24 States Code); and

1 (B) international terrorism (as such term
2 is defined in section 2331(1) of title 18, United
3 States Code).

4 **SEC. 5439. LOCAL LAW ENFORCEMENT SECURITY TRAIN-**
5 **ING.**

6 (a) IN GENERAL.—The Secretary of Homeland Secu-
7 rity, in consultation with public and private sector stake-
8 holders, may in a manner consistent with the protection
9 of privacy rights, civil rights, and civil liberties, develop,
10 through the Federal Law Enforcement Training Centers,
11 a training program to enhance the protection, prepared-
12 ness, and response capabilities of law enforcement agen-
13 cies with respect to threats of terrorism and other threats,
14 including targeted violence, at a surface transportation
15 asset.

16 (b) REQUIREMENTS.—If the Secretary of Homeland
17 Security develops the training program described in sub-
18 section (a), such training program shall—

19 (1) be informed by current information regard-
20 ing tactics used by terrorists and others engaging in
21 targeted violence;

22 (2) include tactical instruction tailored to the
23 diverse nature of the surface transportation asset
24 operational environment; and

1 (3) prioritize training officers from law enforce-
2 ment agencies that are eligible for or receive grants
3 under sections 2003 or 2004 of the Homeland Secu-
4 rity Act of 2002 (6 U.S.C. 604 and 605) and offi-
5 cers employed by railroad carriers that operate pas-
6 senger service, including interstate passenger service.

7 (c) DEFINITIONS.—In this section:

8 (1) The term “public and private sector stake-
9 holders” has the meaning given such term in section
10 114(u)(1)(c) of title 49, United States Code.

11 (2) The term “surface transportation asset” in-
12 cludes facilities, equipment, or systems used to pro-
13 vide transportation services by—

14 (A) a public transportation agency (as
15 such term is defined in section 1402(5) of the
16 Implementing Recommendations of the 9/11
17 Commission Act of 2007 (Public Law 110–53;
18 6 U.S.C. 1131(5)));

19 (B) a railroad carrier (as such term is de-
20 fined in section 20102(3) of title 49, United
21 States Code);

22 (C) an owner or operator of—

23 (i) an entity offering scheduled, fixed-
24 route transportation services by over-the-
25 road bus (as such term is defined in sec-

1 tion 1501(4) of the Implementing Rec-
2 ommendations of the 9/11 Commission Act
3 of 2007 (Public Law 110–53; 6 U.S.C.
4 1151(4)); or

5 (ii) a bus terminal; or

6 (D) other transportation facilities, equip-
7 ment, or systems, as determined by the Sec-
8 retary.

9 (3) The term “targeted violence” means an in-
10 cident of violence in which an attacker selected a
11 particular target in order to inflict mass injury or
12 death with no discernable political or ideological mo-
13 tivation beyond mass injury or death.

14 (4) The term “terrorism” means the terms—

15 (A) domestic terrorism (as such term is de-
16 fined in section 2331(5) of title 18, United
17 States Code); and

18 (B) international terrorism (as such term
19 is defined in section 2331(1) of title 18, United
20 States Code).

21 **SEC. 5440. ALLOWABLE USES OF FUNDS FOR PUBLIC**
22 **TRANSPORTATION SECURITY ASSISTANCE**
23 **GRANTS.**

24 Subparagraph (A) of section 1406(b)(2) of the Imple-
25 menting Recommendations of the 9/11 Commission Act of

1 2007 (6 U.S.C. 1135(b)(2); Public Law 110–53) is
2 amended by inserting “and associated backfill” after “se-
3 curity training”.

4 **SEC. 5441. PERIODS OF PERFORMANCE FOR PUBLIC**
5 **TRANSPORTATION SECURITY ASSISTANCE**
6 **GRANTS.**

7 Section 1406 of the Implementing Recommendations
8 of the 9/11 Commission Act of 2007 (6 U.S.C. 1135; Pub-
9 lic Law 110–53) is amended—

10 (1) by redesignating subsection (m) as sub-
11 section (n); and

12 (2) by inserting after subsection (l) the fol-
13 lowing new subsection:

14 “(m) PERIODS OF PERFORMANCE.—

15 “(1) IN GENERAL.—Except as provided in para-
16 graph (2), funds provided pursuant to a grant
17 awarded under this section for a use specified in
18 subsection (b) shall remain available for use by a
19 grant recipient for a period of not fewer than 36
20 months.

21 “(2) EXCEPTION.—Funds provided pursuant to
22 a grant awarded under this section for a use speci-
23 fied in subparagraph (M) or (N) of subsection (b)(1)
24 shall remain available for use by a grant recipient
25 for a period of not fewer than 55 months.”.

1 **SEC. 5442. GAO REVIEW OF PUBLIC TRANSPORTATION SE-**
2 **CURITY ASSISTANCE GRANT PROGRAM.**

3 (a) IN GENERAL.—The Comptroller General of the
4 United States shall conduct a review of the public trans-
5 portation security assistance grant program under section
6 1406 of the Implementing Recommendations of the 9/11
7 Commission Act of 2007 (6 U.S.C. 1135; Public Law
8 110–53).

9 (b) SCOPE.—The review required under paragraph
10 (1) shall include the following:

11 (1) An assessment of the type of projects fund-
12 ed under the public transportation security grant
13 program referred to in such paragraph.

14 (2) An assessment of the manner in which such
15 projects address threats to public transportation in-
16 frastructure.

17 (3) An assessment of the impact, if any, of sec-
18 tions 5342 through 5345 (including the amendments
19 made by this Act) on types of projects funded under
20 the public transportation security assistance grant
21 program.

22 (4) An assessment of the management and ad-
23 ministration of public transportation security assist-
24 ance grant program funds by grantees.

25 (5) Recommendations to improve the manner in
26 which public transportation security assistance grant

1 program funds address vulnerabilities in public
2 transportation infrastructure.

3 (6) Recommendations to improve the manage-
4 ment and administration of the public transportation
5 security assistance grant program.

6 (c) REPORT.—Not later than one year after the date
7 of the enactment of this Act and again not later than five
8 years after such date of enactment, the Comptroller Gen-
9 eral of the United States shall submit to the Committee
10 on Homeland Security of the House of Representatives
11 and the Committee on Homeland Security and Govern-
12 mental Affairs of the Senate a report on the review re-
13 quired under this section.

14 **SEC. 5443. SENSITIVE SECURITY INFORMATION; INTER-**
15 **NATIONAL AVIATION SECURITY.**

16 (a) SENSITIVE SECURITY INFORMATION.—

17 (1) IN GENERAL.—Not later than 90 days after
18 the date of the enactment of this Act, the Adminis-
19 trator of the Transportation Security Administration
20 (TSA) shall—

21 (A) ensure clear and consistent designation
22 of “Sensitive Security Information”, including
23 reasonable security justifications for such des-
24 ignation;

1 (B) develop and implement a schedule to
2 regularly review and update, as necessary, TSA
3 Sensitive Security Information identification
4 guidelines;

5 (C) develop a tracking mechanism for all
6 Sensitive Security Information redaction and
7 designation challenges;

8 (D) document justifications for changes in
9 position regarding Sensitive Security Informa-
10 tion redactions and designations, and make
11 such changes accessible to TSA personnel for
12 use with relevant stakeholders, including air
13 carriers, airport operators, surface transpor-
14 tation operators, and State and local law en-
15 forcement, as necessary; and

16 (E) ensure that TSA personnel are ade-
17 quately trained on appropriate designation poli-
18 cies.

19 (2) STAKEHOLDER OUTREACH.—Not later than
20 180 days after the date of the enactment of this Act,
21 the Administrator of the Transportation Security
22 Administration (TSA) shall conduct outreach to rel-
23 evant stakeholders described in paragraph (1)(D)
24 that regularly are granted access to Sensitive Secu-
25 rity Information to raise awareness of the TSA's

1 policies and guidelines governing the designation and
2 use of Sensitive Security Information.

3 (b) INTERNATIONAL AVIATION SECURITY.—

4 (1) IN GENERAL.—Not later than 60 days after
5 the date of the enactment of this Act, the Adminis-
6 trator of the Transportation Security Administration
7 shall develop and implement guidelines with respect
8 to last point of departure airports to—

9 (A) ensure the inclusion, as appropriate, of
10 air carriers and other transportation security
11 stakeholders in the development and implemen-
12 tation of security directives and emergency
13 amendments;

14 (B) document input provided by air car-
15 riers and other transportation security stake-
16 holders during the security directive and emer-
17 gency amendment, development, and implemen-
18 tation processes;

19 (C) define a process, including timeframes,
20 and with the inclusion of feedback from air car-
21 riers and other transportation security stake-
22 holders, for cancelling or incorporating security
23 directives and emergency amendments into se-
24 curity programs;

1 (D) conduct engagement with foreign part-
2 ners on the implementation of security direc-
3 tives and emergency amendments, as appro-
4 priate, including recognition if existing security
5 measures at a last point of departure airport
6 are found to provide commensurate security as
7 intended by potential new security directives
8 and emergency amendments; and

9 (E) ensure that new security directives and
10 emergency amendments are focused on defined
11 security outcomes.

12 (2) BRIEFING TO CONGRESS.—Not later than
13 90 days after the date of the enactment of this Act,
14 the Administrator of the Transportation Security
15 Administration shall brief the Committee on Home-
16 land Security of the House of Representatives and
17 the Committee on Commerce, Science, and Trans-
18 portation of the Senate on the guidelines described
19 in paragraph (1).

20 (3) DECISIONS NOT SUBJECT TO JUDICIAL RE-
21 VIEW.—Notwithstanding any other provision of law,
22 any action of the Administrator of the Transpor-
23 tation Security Administration under paragraph (1)
24 is not subject to judicial review.

