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:

TITLE LIV—DEPARTMENT OF HOMELAND SECURITY MEASURES

Subtitle A—DHS Headquarters, Research and Development, and Related Matters

SEC. 5401. CHIEF HUMAN CAPITAL OFFICER RESPONSIBILITIES.

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

(1) in subsection (b)—

(A) in paragraph (1)—

(i) by inserting ", including with respect to leader development and employee engagement," after "policies";

(ii) by striking "and in line" and inserting ", in line"; and

(iii) by inserting ''and informed by best practices within the Federal Government and the private sector,'' after ''priorities,'';

(B) in paragraph (2), by striking ''develop performance measures to provide a basis for monitoring and evaluating'' and inserting ''use performance measures to evaluate, on an ongoing basis,'';

(C) in paragraph (3), by inserting ''that, to the extent practicable, are informed by employee feedback'' after ''policies'';

(D) in paragraph (4), by inserting ''including leader development and employee engagement programs,'' before ''in coordination'';

(E) in paragraph (5), by inserting before the semicolon at the end the following: ''that is informed by an assessment, carried out by the Chief Human Capital Officer, of the learning and developmental needs of employees in supervisory and nonsupervisory roles across the Department and appropriate workforce planning initiatives'';

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

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

''(9) maintain a catalogue of available employee development opportunities, including the Homeland Security Rotation Program pursuant to section 844, departmental leadership development programs, interagency development programs, and other rotational programs;

''(10) ensure that employee discipline and adverse action programs comply with the requirements of all pertinent laws, rules, regulations, and Federal guidance, and ensure due process for employees;

''(11) analyze each Department or Government-wide Federal workforce satisfaction or morale survey not later than 90 days after the date of the publication of each such survey and submit to the Secretary such analysis, including, as appropriate, recommendations to improve workforce satisfaction or morale within the Department;

''(12) review and approve all component employee engagement action plans to ensure such plans include initiatives responsive to the root cause of em-

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

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

(3) by inserting after subsection (c) the following new subsection:

''(d) CHIEF LEARNING AND ENGAGEMENT OFFICER.—The Chief Human Capital Officer may designate an employee of the Department to serve as a Chief Learning and Engagement Officer to assist the Chief Human Capital Officer in carrying out this section.''; and

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

(A) by redesignating paragraphs (2), (3), and (4) as paragraphs (5), (6), and (7), respectively; and

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

''(2) information on employee development opportunities catalogued pursuant to paragraph (9) of subsection (b) and any available data on participation rates, attrition rates, and impacts on retention and employee satisfaction;

''(3) information on the progress of Departmentwide strategic workforce planning efforts as determined under paragraph (2) of subsection (b);

''(4) information on the activities of the steering committee established pursuant to section 711(a), including the number of meetings, types of materials developed and distributed, and recommendations made to the Secretary;''.

SEC. 5402. EMPLOYEE ENGAGEMENT STEERING COMMITTEE AND ACTION PLAN.

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

''SEC. 711. EMPLOYEE ENGAGEMENT.

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

''(1) Identify factors that have a negative impact on employee engagement, morale, and commu-

nications within the Department, such as perceptions about limitations on career progression, mobility, or development opportunities, collected through employee feedback platforms, including through annual employee surveys, questionnaires, and other communications, as appropriate.

''(2) Identify, develop, and distribute initiatives and best practices to improve employee engagement, morale, and communications within the Department, including through annual employee surveys, questionnaires, and other communications, as appropriate.

''(3) Monitor efforts of each component to address employee engagement, morale, and communications based on employee feedback provided through annual employee surveys, questionnaires, and other communications, as appropriate.

''(4) Advise the Secretary on efforts to improve employee engagement, morale, and communications within specific components and across the Department.

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

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

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

''(1) not later than 120 days after the date of the establishment of the employee engagement steering committee under subsection (a), issue a Departmentwide employee engagement action plan, reflecting input from the steering committee and employee feedback provided through annual employee surveys, questionnaires, and other communications in accordance with paragraph (1) of such subsection, to execute strategies to improve employee engagement, morale, and communications within the Department; and

''(2) require the head of each component to—

''(A) develop and implement a component-specific employee engagement plan to advance the action plan required under paragraph (1) that includes performance measures and objectives, is informed by employee feedback provided through annual employee surveys, questionnaires, and other communications, as appropriate, and sets forth how employees and, where applicable, their labor representatives are to be

integrated in developing programs and initiatives;

''(B) monitor progress on implementation of such action plan; and

''(C) provide to the Chief Human Capital Officer and the steering committee quarterly reports on actions planned and progress made under this paragraph.

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

''(d) TERMINATION.—This section shall terminate on the date that is five years after the date of the enactment of this section.''.

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

''Sec. 711. Employee engagement.''.

(c) SUBMISSIONS TO CONGRESS.—

(1) DEPARTMENTWIDE EMPLOYEE ENGAGEMENT ACTION PLAN.—The Secretary of Homeland Security, acting through the Chief Human Capital Officer of the Department of Homeland Security, shall submit to the Committee on Homeland Security of the House of Representatives and the Com-

mittee on Homeland Security and Governmental Affairs of the Senate the Departmentwide employee engagement action plan required under subsection (b)(1) of section 711 of the Homeland Security Act of 2002 (as added by subsection (a) of this section) not later than 30 days after the issuance of such plan under such subsection (b)(1).

(2) COMPONENT-SPECIFIC EMPLOYEE ENGAGEMENT PLANS.—Each head of a component of the Department of Homeland Security shall submit to the Committee on Homeland Security of the House of Representatives and the Committee on Homeland Security and Governmental Affairs of the Senate the component-specific employee engagement plan of each such component required under subsection (b)(2) of section 711 of the Homeland Security Act of 2002 not later than 30 days after the issuance of each such plan under such subsection (b)(2).

SEC. 5403. ANNUAL EMPLOYEE AWARD PROGRAM.

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

"SEC. 712. ANNUAL EMPLOYEE AWARD PROGRAM.

''(a) IN GENERAL.—The Secretary may establish an annual employee award program to recognize Department employees or groups of employees for significant contributions to the achievement of the Department's goals and missions. If such a program is established, the Secretary shall—

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

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

''(3) establish an internal review board comprised of representatives from Department components, headquarters, and field personnel to submit to the Secretary award recommendations regarding specific employees or groups of employees;

''(4) select recipients from the pool of nominees submitted by the internal review board under paragraph (3) and convene a ceremony at which employees or groups of employees receive such awards from the Secretary; and

''(5) publicize such program within the Department.

''(b) INTERNAL REVIEW BOARD.—The internal review board described in subsection (a)(3) shall, when carrying out its function under such subsection, consult with representatives from operational components and headquarters, including supervisory and nonsupervisory personnel, and employee labor organizations that represent Department employees.

''(c) RULE OF CONSTRUCTION.—Nothing in this section may be construed to authorize additional funds to carry out the requirements of this section or to require the Secretary to provide monetary bonuses to recipients of an award under this section.''.

(b) CLERICAL AMENDMENT.—The table of contents in section 1(b) of the Homeland Security Act of 2002, as amended by section 5402 of this Act, is further amended by inserting after the item relating to section 711 the following new item:

''Sec. 712. Annual employee award program.''.

SEC. 5404. INDEPENDENT INVESTIGATION AND IMPLEMENTATION PLAN.

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

similar disciplinary outcomes across the Department for misconduct by a nonsupervisory or supervisor employee who engaged in the same or substantially similar misconduct.

(b) CONSULTATION.—In carrying out the investigation described in subsection (a), the Comptroller General of the United States shall consult with the Under Secretary for Management of the Department of Homeland Security and the employee engagement steering committee established pursuant to subsection (b)(1) of section 711 of the Homeland Security Act of 2002 (as added by section 5302(a) of this Act).

(c) ACTION BY UNDER SECRETARY FOR MANAGEMENT.—Upon completion of the investigation described in subsection (a), the Under Secretary for Management of the Department of Homeland Security shall review the findings and recommendations of such investigation and implement a plan, in consultation with the employee engagement steering committee established pursuant to subsection (b)(1) of section 711 of the Homeland Security Act of 2002, to correct any relevant deficiencies identified by the Comptroller General of the United States in such investigation. The Under Secretary for Management shall direct the employee engagement steering committee to re-

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

SEC. 5405. IMPACTS OF SHUTDOWN.

Not later than 90 days after the date of the enactment of this Act, the Secretary of Homeland Security shall report to the Committee on Homeland Security of the House of Representatives and the Committee on Homeland Security and Governmental Affairs of the Senate regarding the direct and indirect impacts of the lapse in appropriations between December 22, 2018, and January 25, 2019, on—

(1) Department of Homeland Security human resources operations;

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

(3) retention, attrition, and morale of Department personnel.

SEC. 5406. TECHNICAL CORRECTIONS TO QUADRENNIAL HOMELAND SECURITY REVIEW.

(a) IN GENERAL.—Section 707 of the Homeland Security Act of 2002 (6 U.S.C. 347) is amended—

(1) in subsection (a)(3)—

(A) in subparagraph (B), by striking ''and'' after the semicolon at the end;

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

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

''(C) representatives from appropriate advisory committees established pursuant to section 871, including the Homeland Security Advisory Council and the Homeland Security Science and Technology Advisory Committee, or otherwise established, including the Aviation Security Advisory Committee established pursuant to section 44946 of title 49, United States Code; and'';

(2) in subsection (b)—

(A) in paragraph (2), by inserting before the semicolon at the end the following: ''based on the risk assessment required pursuant to subsection (c)(2)(B)'';

(B) in paragraph (3)—

(i) by inserting '', to the extent practicable,'' after ''describe''; and

(ii) by striking ''budget plan'' and inserting ''resources required'';

(C) in paragraph (4)—

(i) by inserting ‘‘, to the extent practicable,’’ after ‘‘identify’’;

(ii) by striking ‘‘budget plan required to provide sufficient resources to successfully’’ and inserting ‘‘resources required to’’; and

(iii) by striking the semicolon at the end and inserting the following: ‘‘, including any resources identified from redundant, wasteful, or unnecessary capabilities or capacities that may be redirected to better support other existing capabilities or capacities, as the case may be; and’’;

(D) in paragraph (5), by striking ‘‘; and’’ and inserting a period; and

(E) by striking paragraph (6);

(3) in subsection (c)—

(A) in paragraph (1), by striking ‘‘December 31 of the year’’ and inserting ‘‘60 days after the date of the submission of the President’s budget for the fiscal year after the fiscal year’’;

(B) in paragraph (2)—

(i) in subparagraph (B), by striking ''description of the threats to'' and inserting ''risk assessment of'';

(ii) in subparagraph (C), by inserting '', as required under subsection (b)(2)'' before the semicolon at the end;

(iii) in subparagraph (D)—

(I) by inserting ''to the extent practicable,'' before ''a description''; and

(II) by striking ''budget plan'' and inserting ''resources required'';

(iv) in subparagraph (F)—

(I) by inserting ''to the extent practicable,'' before ''a discussion''; and

(II) by striking ''the status of'';

(v) in subparagraph (G)—

(I) by inserting ''to the extent practicable,'' before ''a discussion'';

(II) by striking ''the status of'';

(III) by inserting ''and risks'' before ''to national homeland''; and

(IV) by inserting ''and'' after the semicolon at the end;

(vi) by striking subparagraph (H); and

(vii) by redesignating subparagraph (I) as subparagraph (H);

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

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

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

''(A) Records regarding the consultation carried out pursuant to subsection (a)(3), including the following:

''(i) All written communications, including communications sent out by the Secretary and feedback submitted to the Secretary through technology, online communications tools, in-person discussions, and the interagency process.

''(ii) Information on how feedback received by the Secretary informed each such quadrennial homeland security review.

''(B) Information regarding the risk assessment required pursuant to subsection (c)(2)(B), including the following:

''(i) The risk model utilized to generate such risk assessment.

''(ii) Information, including data used in the risk model, utilized to generate such risk assessment.

''(iii) Sources of information, including other risk assessments, utilized to generate such risk assessment.

''(iv) Information on assumptions, weighing factors, and subjective judgments utilized to generate such risk assessment, together with information on the rationale or basis thereof.'';

(4) by redesignating subsection (d) as subsection (e); and

(5) by inserting after subsection (c) the following new subsection:

''(d) REVIEW.—Not later than 90 days after the submission of each report required under subsection (c)(1), the Secretary shall provide to the Committee on Homeland Security of the House of Representatives and the Committee on Homeland Security and Governmental Affairs

of the Senate information on the degree to which the findings and recommendations developed in the quadrennial homeland security review that is the subject of such report were integrated into the acquisition strategy and expenditure plans for the Department.''.

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

SEC. 5407. AUTHORIZATION OF THE ACQUISITION PROFESSIONAL CAREER PROGRAM.

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

''SEC. 713. ACQUISITION PROFESSIONAL CAREER PROGRAM.

''(a) ESTABLISHMENT.—There is established in the Department an acquisition professional career program to develop a cadre of acquisition professionals within the Department.

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

''(c) PROGRAM REQUIREMENTS.—The Under Secretary for Management shall carry out the following with respect to the acquisition professional career program.

''(1) Designate the occupational series, grades, and number of acquisition positions throughout the Department to be included in the program and manage centrally such positions.

''(2) Establish and publish on the Department's website eligibility criteria for candidates to participate in the program.

''(3) Carry out recruitment efforts to attract candidates—

''(A) from institutions of higher education, including such institutions with established acquisition specialties and courses of study, historically Black colleges and universities, and Hispanic-serving institutions;

''(B) with diverse work experience outside of the Federal Government; or

''(C) with military service.

''(4) Hire eligible candidates for designated positions under the program.

''(5) Develop a structured program comprised of acquisition training, on-the-job experience, Departmentwide rotations, mentorship, shadowing, and

other career development opportunities for program participants.

''(6) Provide, beyond required training established for program participants, additional specialized acquisition training, including small business contracting and innovative acquisition techniques training.

''(d) REPORTS.—Not later than December 31, 2021, and annually thereafter through 2027, the Secretary shall submit to the Committee on Homeland Security of the House of Representatives and the Committee on Homeland Security and Governmental Affairs of the Senate a report on the acquisition professional career program. Each such report shall include the following information:

''(1) The number of candidates approved for the program.

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

''(3) A breakdown of the number of participants hired under the program by type of acquisition position.

''(4) A list of Department components and offices that participated in the program and information regarding length of time of each program participant in each rotation at such components or offices.

''(5) Program attrition rates and postprogram graduation retention data, including information on how such data compare to the prior year's data, as available.

''(6) The Department's recruiting efforts for the program.

''(7) The Department's efforts to promote retention of program participants.

''(e) DEFINITIONS.—In this section:

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

''(2) HISTORICALLY BLACK COLLEGES AND UNIVERSITIES.—The term 'historically Black colleges and universities' has the meaning given the term 'part B institution' in section 322(2) of Higher Education Act of 1965 (20 U.S.C. 1061(2)).

''(3) INSTITUTION OF HIGHER EDUCATION.—The term 'institution of higher education' has the

meaning given such term in section 101 of the Higher Education Act of 1965 (20 U.S.C. 1001).''.

(b) CLERICAL AMENDMENT.—The table of contents in section 1(b) of the Homeland Security Act of 2002, as amended by section 5403 of this Act, is further amended by inserting after the item relating to section 712 the following new item:

''Sec. 713. Acquisition professional career program.''.

SEC. 5408. NATIONAL URBAN SECURITY TECHNOLOGY LABORATORY.

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

''SEC. 322. NATIONAL URBAN SECURITY TECHNOLOGY LABORATORY.

''(a) IN GENERAL.—The Secretary, acting through the Under Secretary for Science and Technology, shall designate the laboratory described in subsection (b) as an additional laboratory pursuant to the authority under section 308(c)(2). Such laboratory shall be used to test and evaluate emerging technologies and conduct research and development to assist emergency response providers in preparing for, and protecting against, threats of terrorism.

''(b) LABORATORY DESCRIBED.—The laboratory described in this subsection is the laboratory—

''(1) known, as of the date of the enactment of this section, as the National Urban Security Technology Laboratory; and

''(2) transferred to the Department pursuant to section 303(1)(E).

''(c) LABORATORY ACTIVITIES.—The National Urban Security Technology Laboratory shall—

''(1) conduct tests, evaluations, and assessments of current and emerging technologies, including, as appropriate, the cybersecurity of such technologies that can connect to the internet, for emergency response providers;

''(2) act as a technical advisor to emergency response providers; and

''(3) carry out other such activities as the Secretary determines appropriate.

''(d) RULE OF CONSTRUCTION.—Nothing in this section may be construed as affecting in any manner the authorities or responsibilities of the Countering Weapons of Mass Destruction Office of the Department.''.

(b) CLERICAL AMENDMENT.—The table of contents in section 1(b) of the Homeland Security Act of 2002, as amended by section 5407 of this Act, is further amended by inserting after the item relating to section 321 the following new item:

''Sec. 322. National Urban Security Technology Laboratory.''.

SEC. 5409. DEPARTMENT OF HOMELAND SECURITY BLUE CAMPAIGN ENHANCEMENT.

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

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

(2) by adding at the end the following new subsections:

''(f) WEB-BASED TRAINING PROGRAMS.—To enhance training opportunities, the Director of the Blue Campaign shall develop web-based interactive training videos that utilize a learning management system to provide online training opportunities that shall be made available to the following individuals:

''(1) Federal, State, local, Tribal, and territorial law enforcement officers.

''(2) Non-Federal correction system personnel.

''(3) Such other individuals as the Director determines appropriate.

''(g) BLUE CAMPAIGN ADVISORY BOARD.—

''(1) IN GENERAL.—The Secretary shall establish within the Department a Blue Campaign Advisory Board and shall assign to such Board a representative from each of the following components:

''(A) The Transportation Security Administration.

''(B) U.S. Customs and Border Protection.

''(C) U.S. Immigration and Customs Enforcement.

''(D) The Federal Law Enforcement Training Center.

''(E) The United States Secret Service.

''(F) The Office for Civil Rights and Civil Liberties.

''(G) The Privacy Office.

''(H) Any other components or offices the Secretary determines appropriate.

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

''(A) The Board's mission, goals, and scope of its activities.

''(B) The duties of the Board's representatives.

''(C) The frequency of the Board's meetings.

''(3) CONSULTATION.—The Director shall consult the Board established pursuant to paragraph (1) regarding the following:

''(A) Recruitment tactics used by human traffickers to inform the development of training and materials by the Blue Campaign.

''(B) The development of effective awareness tools for distribution to Federal and non-Federal officials to identify and prevent instances of human trafficking.

''(C) Identification of additional persons or entities that may be uniquely positioned to recognize signs of human trafficking and the development of materials for such persons.

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

''(A) the Board; or

''(B) consultations under paragraph (2).

''(h) CONSULTATION.—With regard to the development of programs under the Blue Campaign and the implementation of such programs, the Director is authorized to consult with State, local, Tribal, and territorial agencies, nongovernmental organizations, private sector organizations, and experts. Such consultation shall be exempt from the Federal Advisory Committee Act (5 U.S.C. App.).''.

SEC. 5410. DEPARTMENT OF HOMELAND SECURITY MENTOR-PROTÉGÉ PROGRAM.

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

"SEC. 890B. MENTOR-PROTÉGÉ PROGRAM.

''(a) ESTABLISHMENT.—There is established in the Department a mentor-protégé program (in this section referred to as the 'Program') under which a mentor firm enters into an agreement with a protégé firm for the purpose of assisting the protégé firm to compete for prime contracts and subcontracts of the Department.

''(b) ELIGIBILITY.—The Secretary shall establish criteria for mentor firms and protégé firms to be eligible to participate in the Program, including a requirement that a firm is not included on any list maintained by the Federal Government of contractors that have been suspended or debarred.

''(c) PROGRAM APPLICATION AND APPROVAL.—

''(1) APPLICATION.—The Secretary, acting through the Office of Small and Disadvantaged Business Utilization of the Department, shall establish a process for submission of an application jointly by a mentor firm and the protégé firm selected by the mentor firm. The application shall include each of the following:

"(A) A description of the assistance to be provided by the mentor firm, including, to the extent available, the number and a brief description of each anticipated subcontract to be awarded to the protégé firm.

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

"(C) An estimate of the costs to be incurred by the mentor firm for providing assistance under the Program.

"(D) Attestations that Program participants will submit to the Secretary reports at times specified by the Secretary to assist the Secretary in evaluating the protégé firm's developmental progress.

"(E) Attestations that Program participants will inform the Secretary in the event of a change in eligibility or voluntary withdrawal from the Program.

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

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

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

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

''(e) PROGRAM BENEFITS.—A mentor firm and protégé firm that enter into an agreement under subsection (d) may receive the following Program benefits:

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

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

''(3) A protégé firm may receive technical, managerial, financial, or any other mutually agreed upon benefit from a mentor firm, including a subcontract award.

''(f) REPORTING.—Not later than one year after the date of the enactment of this Act, and annually thereafter, the head of the Office of Small and Disadvantaged Business Utilization shall submit to the Committee on Homeland Security and Governmental Affairs and the Committee on Small Business and Entrepreneurship of the Senate and the Committee on Homeland Security and the Committee on Small Business of the House of Representatives a report that—

''(1) identifies each agreement between a mentor firm and a protégé firm entered into under this section, including the number of protégé firm participants that are—

''(A) small business concerns;

''(B) small business concerns owned and controlled by veterans;

''(C) small business concerns owned and controlled by service-disabled veterans;

''(D) qualified HUBZone small business concerns;

''(E) small business concerns owned and controlled by socially and economically disadvantaged individuals;

''(F) small business concerns owned and controlled by women;

''(G) historically Black colleges and universities; and

''(H) minority institutions of higher education;

''(2) describes the type of assistance provided by mentor firms to protégé firms;

''(3) identifies contracts within the Department in which a mentor firm serving as the prime contractor provided subcontracts to a protégé firm under the Program; and

''(4) assesses the degree to which there has been—

''(A) an increase in the technical capabilities of protégé firms; and

''(B) an increase in the quantity and estimated value of prime contract and subcontract awards to protégé firms for the period covered by the report.

''(g) RULE OF CONSTRUCTION.—Nothing in this section may be construed to limit, diminish, impair, or other-

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

''(h) DEFINITIONS.—In this section:

''(1) HISTORICALLY BLACK COLLEGE OR UNIVERSITY.—The term 'historically Black college or university' means any of the historically Black colleges and universities referred to in section 2323 of title 10, United States Code, as in effect on March 1, 2018.

''(2) MENTOR FIRM.—The term 'mentor firm' means a for-profit business concern that is not a small business concern that—

''(A) has the ability to assist and commits to assisting a protégé firm to compete for Federal prime contracts and subcontracts; and

''(B) satisfies any other requirements imposed by the Secretary.

''(3) MINORITY INSTITUTION OF HIGHER EDUCATION.—The term 'minority institution of higher

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

''(4) PROTÉGÉ FIRM.—The term 'protégé firm' means a small business concern, a historically Black college or university, or a minority institution of higher education that—

''(A) is eligible to enter into a prime contract or subcontract with the Department; and

''(B) satisfies any other requirements imposed by the Secretary.

''(5) SMALL BUSINESS ACT DEFINITIONS.—The terms 'small business concern', 'small business concern owned and controlled by veterans', 'small business concern owned and controlled by service-disabled veterans', 'qualified HUBZone small business concern', and 'small business concern owned and controlled by women' have the meanings given such terms, respectively, under section 3 of the Small Business Act (15 U.S.C. 632). The term 'small business concern owned and controlled by socially and economically disadvantaged individuals' has the meaning given such term in section 8(d)(3)(C) of the Small Business Act (15 U.S.C. 637(d)(3)(C)).''.

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

''Sec. 890B. Mentor-protégé program.''.

SEC. 5411. MEDICAL COUNTERMEASURES PROGRAM.

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

''SEC. 1932. MEDICAL COUNTERMEASURES.

''(a) IN GENERAL.—The Secretary shall establish a medical countermeasures program to facilitate personnel readiness, and protection for the Department's employees and working animals in the event of a chemical, biological, radiological, nuclear, or explosives attack, naturally occurring disease outbreak, or pandemic, and to support Department mission continuity.

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

''(1) develop Departmentwide standards for medical countermeasure storage, security, dispensing, and documentation;

''(2) maintain a stockpile of medical countermeasures, including antibiotics, antivirals, and radiological countermeasures, as appropriate;

''(3) preposition appropriate medical countermeasures in strategic locations nationwide, based on threat and employee density, in accordance with applicable Federal statutes and regulations;

''(4) provide oversight and guidance regarding the dispensing of stockpiled medical countermeasures;

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

''(6) provide training to Department employees on medical countermeasure dispensing; and

''(7) support dispensing exercises.

''(c) MEDICAL COUNTERMEASURES WORKING GROUP.—The Chief Medical Officer shall establish a medical countermeasures working group comprised of representatives from appropriate components and offices of the Department to ensure that medical countermeasures standards are maintained and guidance is consistent.

''(d) MEDICAL COUNTERMEASURES MANAGEMENT.—Not later than 120 days after the date of the en-

actment of this section, the Chief Medical Officer shall develop and submit to the Secretary an integrated logistics support plan for medical countermeasures, including—

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

''(2) a replenishment plan; and

''(3) inventory tracking, reporting, and reconciliation procedures for existing stockpiles and new medical countermeasure purchases.

''(e) STOCKPILE ELEMENTS.—In determining the types and quantities of medical countermeasures to stockpile under subsection (d), the Chief Medical Officer shall utilize, if available—

''(1) Department chemical, biological, radiological, and nuclear risk assessments; and

''(2) Centers for Disease Control and Prevention guidance on medical countermeasures.

''(f) REPORT.—Not later than 180 days after the date of the enactment of this section, the Secretary shall submit to the Committee on Homeland Security of the House of Representatives and the Committee on Homeland Security and Governmental Affairs of the Senate the plan developed in accordance with subsection (d) and brief

such Committees regarding implementing the requirements of this section.

''(g) DEFINITION.—In this section, the term 'medical countermeasures' means antibiotics, antivirals, radiological countermeasures, and other countermeasures that may be deployed to protect the Department's employees and working animals in the event of a chemical, biological, radiological, nuclear, or explosives attack, naturally occurring disease outbreak, or pandemic.''.

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

''Sec. 1932. Medical countermeasures.''.

SEC. 5412. CRITICAL DOMAIN RESEARCH AND DEVELOPMENT.

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

''SEC. 890C. HOMELAND SECURITY CRITICAL DOMAIN RESEARCH AND DEVELOPMENT.

''(a) IN GENERAL.—

''(1) RESEARCH AND DEVELOPMENT.—The Secretary is authorized to conduct research and development to—

''(A) identify United States critical domains for economic security and homeland security; and

''(B) evaluate the extent to which disruption, corruption, exploitation, or dysfunction of any of such domain poses a substantial threat to homeland security.

''(2) REQUIREMENTS.—

''(A) RISK ANALYSIS OF CRITICAL DOMAINS.—The research under paragraph (1) shall include a risk analysis of each identified United States critical domain for economic security to determine the degree to which there exists a present or future threat to homeland security in the event of disruption, corruption, exploitation, or dysfunction to such domain. Such research shall consider, to the extent possible, the following:

''(i) The vulnerability and resilience of relevant supply chains.

''(ii) Foreign production, processing, and manufacturing methods.

''(iii) Influence of malign economic actors.

''(iv) Asset ownership.

''(v) Relationships within the supply chains of such domains.

''(vi) The degree to which the conditions referred to in clauses (i) through (v) would place such a domain at risk of disruption, corruption, exploitation, or dysfunction.

''(B) ADDITIONAL RESEARCH INTO HIGH-RISK CRITICAL DOMAINS.—Based on the identification and risk analysis of United States critical domains for economic security pursuant to paragraph (1) and subparagraph (A) of this paragraph, respectively, the Secretary may conduct additional research into those critical domains, or specific elements thereof, with respect to which there exists the highest degree of a present or future threat to homeland security in the event of disruption, corruption, exploitation, or dysfunction to such a domain. For each such high-risk domain, or element thereof, such research shall—

''(i) describe the underlying infrastructure and processes;

''(ii) analyze present and projected performance of industries that comprise or support such domain;

''(iii) examine the extent to which the supply chain of a product or service necessary to such domain is concentrated, either through a small number of sources, or if multiple sources are concentrated in one geographic area;

''(iv) examine the extent to which the demand for supplies of goods and services of such industries can be fulfilled by present and projected performance of other industries, identify strategies, plans, and potential barriers to expand the supplier industrial base, and identify the barriers to the participation of such other industries;

''(v) consider each such domain's performance capacities in stable economic environments, adversarial supply conditions, and under crisis economic constraints;

''(vi) identify and define needs and requirements to establish supply resiliency within each such domain; and

''(vii) consider the effects of sector consolidation, including foreign consolidation, either through mergers or acquisitions, or due to recent geographic realignment, on such industries' performances.

''(3) CONSULTATION.—In conducting the research under paragraph (1) and subparagraph (B) of paragraph (2), the Secretary may consult with appropriate Federal agencies, State agencies, and private sector stakeholders.

''(4) PUBLICATION.—Beginning one year after the date of the enactment of this section, the Secretary shall publish a report containing information relating to the research under paragraph (1) and subparagraph (B) of paragraph (2), including findings, evidence, analysis, and recommendations. Such report shall be updated annually through 2026.

''(b) SUBMISSION TO CONGRESS.—Not later than 90 days after the publication of each report required under paragraph (4) of subsection (a), the Secretary shall transmit to the Committee on Homeland Security of the House of Representatives and the Committee on Homeland Secu-

rity and Governmental Affairs of the Senate each such report, together with a description of actions the Secretary, in consultation with appropriate Federal agencies, will undertake or has undertaken in response to each such report.

''(c) DEFINITIONS.—In this section:

''(1) UNITED STATES CRITICAL DOMAINS FOR ECONOMIC SECURITY.—The term 'United States critical domains for economic security' means the critical infrastructure and other associated industries, technologies, and intellectual property, or any combination thereof, that are essential to the economic security of the United States.

''(2) ECONOMIC SECURITY.—The term 'economic security' means the condition of having secure and resilient domestic production capacity, combined with reliable access to the global resources necessary to maintain an acceptable standard of living and to protect core national values.

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

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

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

''Sec. 890C. Homeland security critical domain research and development.''.

Subtitle B—Cybersecurity

SEC. 5421. TITLE XXII TECHNICAL AND CLERICAL AMENDMENTS.

(a) TECHNICAL AMENDMENTS.—

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

(A) in the first section 2215 (6 U.S.C. 665; relating to the duties and authorities relating to .gov internet domain), by amending the section enumerator and heading to read as follows:

''SEC. 2215. DUTIES AND AUTHORITIES RELATING TO .GOV INTERNET DOMAIN.'';

(B) in the second section 2215 (6 U.S.C. 665b; relating to the joint cyber planning office), by amending the section enumerator and heading to read as follows:

''SEC. 2216. JOINT CYBER PLANNING OFFICE.'';

(C) in the third section 2215 (6 U.S.C. 665c; relating to the Cybersecurity State Coordinator), by amending the section enumerator and heading to read as follows:

"SEC. 2217. CYBERSECURITY STATE COORDINATOR.";

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

"SEC. 2218. SECTOR RISK MANAGEMENT AGENCIES.";

(E) in section 2216 (6 U.S.C. 665e; relating to the Cybersecurity Advisory Committee), by amending the section enumerator and heading to read as follows:

"SEC. 2219. CYBERSECURITY ADVISORY COMMITTEE."; and

(F) in section 2217 (6 U.S.C. 665f; relating to Cybersecurity Education and Training Programs), by amending the section enumerator and heading to read as follows:

"SEC. 2220. CYBERSECURITY EDUCATION AND TRAINING PROGRAMS.".

(2) CONSOLIDATED APPROPRIATIONS ACT, 2021.—Paragraph (1) of section 904(b) of division U of the Consolidated Appropriations Act, 2021 (Public Law 116–260) is amended, in the matter preceding subparagraph (A), by inserting ''of 2002'' after ''Homeland Security Act''.

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

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

SEC. 5422. STATE AND LOCAL CYBERSECURITY GRANT PROGRAM.

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

''SEC. 2220A. STATE AND LOCAL CYBERSECURITY GRANT PROGRAM.

''(a) DEFINITIONS.—In this section:

''(1) CYBER THREAT INDICATOR.—The term 'cyber threat indicator' has the meaning given the term in section 102 of the Cybersecurity Act of 2015 (6 U.S.C. 1501).

''(2) CYBERSECURITY PLAN.—The term 'Cybersecurity Plan' means a plan submitted by an eligible entity under subsection (e)(1).

''(3) ELIGIBLE ENTITY.—The term 'eligible entity' means—

''(A) a State; or

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

''(i) notifies the Secretary that the Indian Tribe intends to develop a Cybersecurity Plan; and

''(ii) agrees to forfeit any distribution under subsection (n)(2).

''(4) INCIDENT.—The term 'incident' has the meaning given the term in section 2209.

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

''(6) INFORMATION SHARING AND ANALYSIS ORGANIZATION.—The term 'information sharing and analysis organization' has the meaning given the term in section 2222.

''(7) INFORMATION SYSTEM.—The term 'information system' has the meaning given the term in section 102 of the Cybersecurity Act of 2015 (6 U.S.C. 1501).

''(8) ONLINE SERVICE.—The term 'online service' means any internet-facing service, including a website, email, virtual private network, or custom application.

''(9) RANSOMWARE INCIDENT.—The term 'ransomware incident' means an incident that actually or imminently jeopardizes, without lawful authority, the integrity, confidentiality, or availability of information on an information system, or actually or imminently jeopardizes, without lawful authority, an information system for the purpose of coercing the information system's owner, operator, or another person.

''(10) STATE AND LOCAL CYBERSECURITY GRANT PROGRAM.—The term 'State and Local Cybersecurity Grant Program' means the program established under subsection (b).

''(11) STATE AND LOCAL CYBERSECURITY RESILIENCE COMMITTEE.—The term 'State and Local Cybersecurity Resilience Committee' means the committee established under subsection (o)(1).

''(12) TRIBAL ORGANIZATION.—The term 'Tribal organization' has the meaning given such term in section 4(l) of the of the Indian Self-Determination and Education Assistance Act (25 U.S.C. 5304(l)).

''(b) ESTABLISHMENT.—

''(1) IN GENERAL.—The Secretary, acting through the Director, shall establish a program, to be known as the 'the State and Local Cybersecurity Grant Program', to award grants to eligible entities to address cybersecurity risks and cybersecurity threats to information systems of State, local, or Tribal organizations.

''(2) APPLICATION.—An eligible entity seeking a grant under the State and Local Cybersecurity Grant Program shall submit to the Secretary an application at such time, in such manner, and containing such information as the Secretary may require.

''(c) BASELINE REQUIREMENTS.—An eligible entity or multistate group that receives a grant under this section shall use the grant in compliance with—

''(1)(A) the Cybersecurity Plan of the eligible entity or the Cybersecurity Plans of the eligible entities that comprise the multistate group; and

''(B) the Homeland Security Strategy to Improve the Cybersecurity of State, Local, Tribal, and Territorial Governments developed under section 2210(e)(1); or

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

''(d) ADMINISTRATION.—The State and Local Cybersecurity Grant Program shall be administered in the same office of the Department that administers grants made under sections 2003 and 2004.

''(e) CYBERSECURITY PLANS.—

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

''(2) REQUIRED ELEMENTS.—A Cybersecurity Plan of an eligible entity shall—

''(A) incorporate, to the extent practicable, any existing plans of the eligible entity to protect against cybersecurity risks and cybersecurity threats to information systems of State, local, or Tribal organizations;

''(B) describe, to the extent practicable, how the eligible entity will—

''(i) manage, monitor, and track information systems, applications, and user accounts owned or operated by or on behalf of the eligible entity or by local or Tribal organizations within the jurisdiction of the eligible entity and the information tech-

nology deployed on those information systems, including legacy information systems and information technology that are no longer supported by the manufacturer of the systems or technology;

''(ii) monitor, audit, and track activity between information systems, applications, and user accounts owned or operated by or on behalf of the eligible entity or by local or Tribal organizations within the jurisdiction of the eligible entity and between those information systems and information systems not owned or operated by the eligible entity or by local or Tribal organizations within the jurisdiction of the eligible entity;

''(iii) enhance the preparation, response, and resilience of information systems, applications, and user accounts owned or operated by or on behalf of the eligible entity or local or Tribal organizations against cybersecurity risks and cybersecurity threats;

''(iv) implement a process of continuous cybersecurity vulnerability assess-

ments and threat mitigation practices prioritized by degree of risk to address cybersecurity risks and cybersecurity threats on information systems of the eligible entity or local or Tribal organizations;

''(v) ensure that State, local, and Tribal organizations that own or operate information systems that are located within the jurisdiction of the eligible entity—

''(I) adopt best practices and methodologies to enhance cybersecurity, such as the practices set forth in the cybersecurity framework developed by, and the cyber supply chain risk management best practices identified by, the National Institute of Standards and Technology; and

''(II) utilize knowledge bases of adversary tools and tactics to assess risk;

''(vi) promote the delivery of safe, recognizable, and trustworthy online services by State, local, and Tribal organizations, including through the use of the .gov internet domain;

''(vii) ensure continuity of operations of the eligible entity and local, and Tribal organizations in the event of a cybersecurity incident (including a ransomware incident), including by conducting exercises to practice responding to such an incident;

''(viii) use the National Initiative for Cybersecurity Education Cybersecurity Workforce Framework developed by the National Institute of Standards and Technology to identify and mitigate any gaps in the cybersecurity workforces of State, local, or Tribal organizations, enhance recruitment and retention efforts for such workforces, and bolster the knowledge, skills, and abilities of State, local, and Tribal organization personnel to address cybersecurity risks and cybersecurity threats, such as through cybersecurity hygiene training;

''(ix) ensure continuity of communications and data networks within the jurisdiction of the eligible entity between the eligible entity and local and Tribal organizations that own or operate information sys-

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

''(x) assess and mitigate, to the greatest degree possible, cybersecurity risks and cybersecurity threats related to critical infrastructure and key resources, the degradation of which may impact the performance of information systems within the jurisdiction of the eligible entity;

''(xi) enhance capabilities to share cyber threat indicators and related information between the eligible entity and local and Tribal organizations that own or operate information systems within the jurisdiction of the eligible entity, including by expanding existing information-sharing agreements with the Department;

''(xii) enhance the capability of the eligible entity to share cyber threat indictors and related information with the Department;

''(xiii) leverage cybersecurity services offered by the Department;

"(xiv) develop and coordinate strategies to address cybersecurity risks and cybersecurity threats to information systems of the eligible entity in consultation with—

"(I) local and Tribal organizations within the jurisdiction of the eligible entity; and

"(II) as applicable—

"(aa) States that neighbor the jurisdiction of the eligible entity or, as appropriate, members of an information sharing and analysis organization; and

"(bb) countries that neighbor the jurisdiction of the eligible entity; and

"(xv) implement an information technology and operational technology modernization cybersecurity review process that ensures alignment between information technology and operational technology cybersecurity objectives;

"(C) describe, to the extent practicable, the individual responsibilities of the eligible entity and local and Tribal organizations within the

jurisdiction of the eligible entity in implementing the plan;

''(D) outline, to the extent practicable, the necessary resources and a timeline for implementing the plan; and

''(E) describe how the eligible entity will measure progress toward implementing the plan.

''(3) DISCRETIONARY ELEMENTS.—A Cybersecurity Plan of an eligible entity may include a description of—

''(A) cooperative programs developed by groups of local and Tribal organizations within the jurisdiction of the eligible entity to address cybersecurity risks and cybersecurity threats; and

''(B) programs provided by the eligible entity to support local and Tribal organizations and owners and operators of critical infrastructure to address cybersecurity risks and cybersecurity threats.

''(4) MANAGEMENT OF FUNDS.—An eligible entity applying for a grant under this section shall agree to designate the Chief Information Officer, the Chief Information Security Officer, or an equivalent

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

''(f) MULTISTATE GRANTS.—

''(1) IN GENERAL.—The Secretary, acting through the Director, may award grants under this section to a group of two or more eligible entities to support multistate efforts to address cybersecurity risks and cybersecurity threats to information systems within the jurisdictions of the eligible entities.

''(2) SATISFACTION OF OTHER REQUIREMENTS.—In order to be eligible for a multistate grant under this subsection, each eligible entity that comprises a multistate group shall submit to the Secretary—

''(A) a Cybersecurity Plan for approval in accordance with subsection (i); and

''(B) a plan for establishing a cybersecurity planning committee under subsection (g).

''(3) APPLICATION.—

''(A) IN GENERAL.—A multistate group applying for a multistate grant under paragraph (1) shall submit to the Secretary an application at such time, in such manner, and

containing such information as the Secretary may require.

''(B) MULTISTATE PROJECT DESCRIPTION.—An application of a multistate group under subparagraph (A) shall include a plan describing—

''(i) the division of responsibilities among the eligible entities that comprise the multistate group for administering the grant for which application is being made;

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

''(iii) how the eligible entities that comprise the multistate group will work together to implement the Cybersecurity Plan of each of those eligible entities.

''(g) PLANNING COMMITTEES.—

''(1) IN GENERAL.—An eligible entity that receives a grant under this section shall establish a cybersecurity planning committee to—

''(A) assist in the development, implementation, and revision of the Cybersecurity Plan of the eligible entity;

''(B) approve the Cybersecurity Plan of the eligible entity; and

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

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

''(A) be comprised of representatives from the eligible entity and counties, cities, towns, Tribes, and public educational and health institutions within the jurisdiction of the eligible entity; and

''(B) include, as appropriate, representatives of rural, suburban, and high-population jurisdictions.

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

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

a multijurisdictional planning committee or commission that meets, or may be leveraged to meet, the requirements of this subsection.

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

''(1) implement the Cybersecurity Plan of the eligible entity;

''(2) develop or revise the Cybersecurity Plan of the eligible entity; or

''(3) assist with activities that address imminent cybersecurity risks or cybersecurity threats to the information systems of the eligible entity or a local or Tribal organization within the jurisdiction of the eligible entity.

''(i) APPROVAL OF PLANS.—

''(1) APPROVAL AS CONDITION OF GRANT.—Before an eligible entity may receive a grant under this section, the Secretary, acting through the Director, shall review the Cybersecurity Plan, or any revisions thereto, of the eligible entity and approve such plan, or revised plan, if it satisfies the requirements specified in paragraph (2).

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

subsection, the Director shall ensure that the Cybersecurity Plan—

''(A) satisfies the requirements of subsection (e)(2);

''(B) upon the issuance of the Homeland Security Strategy to Improve the Cybersecurity of State, Local, Tribal, and Territorial Governments authorized pursuant to section 2210(e), complies, as appropriate, with the goals and objectives of the strategy; and

''(C) has been approved by the cybersecurity planning committee of the eligible entity established under subsection (g).

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

''(4) EXCEPTION.—Notwithstanding subsection (e) and paragraph (1) of this subsection, the Secretary may award a grant under this section to an eligible entity that does not submit a Cybersecurity Plan to the Secretary if—

''(A) the eligible entity certifies to the Secretary that—

''(i) the activities that will be supported by the grant are integral to the development of the Cybersecurity Plan of the eligible entity; and

''(ii) the eligible entity will submit by September 30, 2023, to the Secretary, a Cybersecurity Plan for review, and if appropriate, approval; or

''(B) the eligible entity certifies to the Secretary, and the Director confirms, that the eligible entity will use funds from the grant to assist with the activities described in subsection (h)(3).

''(j) LIMITATIONS ON USES OF FUNDS.—

''(1) IN GENERAL.—An eligible entity that receives a grant under this section may not use the grant—

''(A) to supplant State, local, or Tribal funds;

''(B) for any recipient cost-sharing contribution;

''(C) to pay a demand for ransom in an attempt to—

''(i) regain access to information or an information system of the eligible entity

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

''(ii) prevent the disclosure of information that has been removed without authorization from an information system of the eligible entity or of a local or Tribal organization within the jurisdiction of the eligible entity;

''(D) for recreational or social purposes; or

''(E) for any purpose that does not address cybersecurity risks or cybersecurity threats on information systems of the eligible entity or of a local or Tribal organization within the jurisdiction of the eligible entity.

''(2) PENALTIES.—In addition to any other remedy available, the Secretary may take such actions as are necessary to ensure that a recipient of a grant under this section uses the grant for the purposes for which the grant is awarded.

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

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

''(k) OPPORTUNITY TO AMEND APPLICATIONS.—In considering applications for grants under this section, the Secretary shall provide applicants with a reasonable opportunity to correct defects, if any, in such applications before making final awards.

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

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

''(2) REMAINDER.—The Secretary shall apportion the remainder of such amounts in the ratio that—

''(A) the population of each eligible entity, bears to

''(B) the population of all eligible entities.

''(3) MINIMUM ALLOCATION TO INDIAN TRIBES.—

''(A) IN GENERAL.—In apportioning amounts under this section, the Secretary shall ensure that, for each fiscal year, directly eligible Tribes collectively receive, from amounts appropriated under the State and Local Cybersecurity Grant Program, not less than an amount equal to three percent of the total amount appropriated for grants under this section.

''(B) ALLOCATION.—Of the amount reserved under subparagraph (A), funds shall be allocated in a manner determined by the Secretary in consultation with Indian Tribes.

''(C) EXCEPTION.—This paragraph shall not apply in any fiscal year in which the Secretary—

''(i) receives fewer than five applications from Indian Tribes; or

''(ii) does not approve at least two applications from Indian Tribes.

''(m) FEDERAL SHARE.—

''(1) IN GENERAL.—The Federal share of the cost of an activity carried out using funds made available with a grant under this section may not exceed—

''(A) in the case of a grant to an eligible entity—

''(i) for fiscal year 2022, 90 percent;

''(ii) for fiscal year 2023, 80 percent;

''(iii) for fiscal year 2024, 70 percent;

''(iv) for fiscal year 2025, 60 percent; and

''(v) for fiscal year 2026 and each subsequent fiscal year, 50 percent; and

''(B) in the case of a grant to a multistate group—

''(i) for fiscal year 2022, 95 percent;

''(ii) for fiscal year 2023, 85 percent;

''(iii) for fiscal year 2024, 75 percent;

''(iv) for fiscal year 2025, 65 percent; and

''(v) for fiscal year 2026 and each subsequent fiscal year, 55 percent.

''(2) WAIVER.—The Secretary may waive or modify the requirements of paragraph (1) for an Indian Tribe if the Secretary determines such a waiver is in the public interest.

''(n) RESPONSIBILITIES OF GRANTEES.—

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

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

''(A) for the purpose for which the grant is awarded; and

''(B) in compliance with, as the case may be—

''(i) the Cybersecurity Plan of the eligible entity;

''(ii) the Cybersecurity Plans of the eligible entities that comprise the multistate group; or

''(iii) a purpose approved by the Secretary under subsection (h) or pursuant to an exception under subsection (i).

''(2) AVAILABILITY OF FUNDS TO LOCAL AND TRIBAL ORGANIZATIONS.—Not later than 45 days after the date on which an eligible entity or multistate group receives a grant under this section, the eligible entity or multistate group shall, without imposing unreasonable or unduly burdensome requirements as a condition of receipt, obligate or otherwise make available to local and Tribal organizations within the jurisdiction of the eligible entity or the eligible entities that comprise the multistate group, and as applicable, consistent with the Cyber-

security Plan of the eligible entity or the Cybersecurity Plans of the eligible entities that comprise the multistate group—

"(A) not less than 80 percent of funds available under the grant;

"(B) with the consent of the local and Tribal organizations, items, services, capabilities, or activities having a value of not less than 80 percent of the amount of the grant; or

"(C) with the consent of the local and Tribal organizations, grant funds combined with other items, services, capabilities, or activities having the total value of not less than 80 percent of the amount of the grant.

"(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).

"(4) EXTENSION OF PERIOD.—

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

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

''(B) APPROVAL.—The Secretary may approve a request for an extension under subparagraph (A) if the Secretary determines the extension is necessary to ensure that the obligation and expenditure of grant funds align with the purpose of the State and Local Cybersecurity Grant Program.

''(5) EXCEPTION.—Paragraph (2) shall not apply to the District of Columbia, the Commonwealth of Puerto Rico, American Samoa, the Commonwealth of the Northern Mariana Islands, Guam, the United States Virgin Islands, or an Indian Tribe.

''(6) DIRECT FUNDING.—If an eligible entity does not make a distribution to a local or Tribal organization required in accordance with paragraph (2), the local or Tribal organization may petition the Secretary to request that grant funds be provided directly to the local or Tribal organization.

''(7) PENALTIES.—In addition to other remedies available to the Secretary, the Secretary may terminate or reduce the amount of a grant awarded under this section to an eligible entity or distribute

grant funds previously awarded to such eligible entity directly to the appropriate local or Tribal organization as a replacement grant in an amount the Secretary determines appropriate if such eligible entity violates a requirement of this subsection.

''(o) ADVISORY COMMITTEE.—

''(1) ESTABLISHMENT.—Not later than 120 days after the date of enactment of this section, the Director shall establish a State and Local Cybersecurity Resilience Committee to provide State, local, and Tribal stakeholder expertise, situational awareness, and recommendations to the Director, as appropriate, regarding how to—

''(A) address cybersecurity risks and cybersecurity threats to information systems of State, local, or Tribal organizations; and

''(B) improve the ability of State, local, and Tribal organizations to prevent, protect against, respond to, mitigate, and recover from such cybersecurity risks and cybersecurity threats.

''(2) DUTIES.—The committee established under paragraph (1) shall—

"(A) submit to the Director recommendations that may inform guidance for applicants for grants under this section;

"(B) upon the request of the Director, provide to the Director technical assistance to inform the review of Cybersecurity Plans submitted by applicants for grants under this section, and, as appropriate, submit to the Director recommendations to improve those plans prior to the approval of the plans under subsection (i);

"(C) advise and provide to the Director input regarding the Homeland Security Strategy to Improve Cybersecurity for State, Local, Tribal, and Territorial Governments required under section 2210;

"(D) upon the request of the Director, provide to the Director recommendations, as appropriate, regarding how to—

"(i) address cybersecurity risks and cybersecurity threats on information systems of State, local, or Tribal organizations; and

"(ii) improve the cybersecurity resilience of State, local, or Tribal organizations; and

"(E) regularly coordinate with the State, Local, Tribal and Territorial Government Coordinating Council, within the Critical Infrastructure Partnership Advisory Council, established under section 871.

"(3) MEMBERSHIP.—

"(A) NUMBER AND APPOINTMENT.—The State and Local Cybersecurity Resilience Committee established pursuant to paragraph (1) shall be composed of 15 members appointed by the Director, as follows:

"(i) Two individuals recommended to the Director by the National Governors Association.

"(ii) Two individuals recommended to the Director by the National Association of State Chief Information Officers.

"(iii) One individual recommended to the Director by the National Guard Bureau.

''(iv) Two individuals recommended to the Director by the National Association of Counties.

''(v) One individual recommended to the Director by the National League of Cities.

''(vi) One individual recommended to the Director by the United States Conference of Mayors.

''(vii) One individual recommended to the Director by the Multi-State Information Sharing and Analysis Center.

''(viii) One individual recommended to the Director by the National Congress of American Indians.

''(viii) Four individuals who have educational and professional experience relating to cybersecurity work or cybersecurity policy.

''(B) TERMS.—

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

''(ii) REQUIREMENT.—At least two members of the State and Local Cybersecurity Resilience Committee shall also be members of the State, Local, Tribal and Territorial Government Coordinating Council, within the Critical Infrastructure Partnership Advisory Council, established under section 871.

''(iii) EXCEPTION.—A term of a member of the State and Local Cybersecurity Resilience Committee shall be three years if the member is appointed initially to the Committee upon the establishment of the Committee.

''(iv) TERM REMAINDERS.—Any member of the State and Local Cybersecurity Resilience Committee appointed to fill a vacancy occurring before the expiration of the term for which the member's predecessor was appointed shall be appointed only for the remainder of such term. A member may serve after the expiration of such member's term until a successor has taken office.

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

''(C) PAY.—Members of the State and Local Cybersecurity Resilience Committee shall serve without pay.

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

''(5) PERMANENT AUTHORITY.—Notwithstanding section 14 of the Federal Advisory Committee Act (5 U.S.C. App.), the State and Local Cybersecurity Resilience Committee shall be a permanent authority.

''(p) REPORTS.—

''(1) ANNUAL REPORTS BY GRANT RECIPIENTS.—

''(A) IN GENERAL.—Not later than one year after an eligible entity or multistate group receives funds under this section, the eligible entity or multistate group shall submit to the Secretary a report on the progress of the eligible entity or multistate group in implementing

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

''(B) ABSENCE OF PLAN.—Not later than 180 days after an eligible entity that does not have a Cybersecurity Plan receives funds under this section for developing its Cybersecurity Plan, the eligible entity shall submit to the Secretary a report describing how the eligible entity obligated and expended grant funds during the fiscal year to—

''(i) so develop such a Cybersecurity Plan; or

''(ii) assist with the activities described in subsection (h)(3).

''(2) ANNUAL REPORTS TO CONGRESS.—Not less frequently than once per year, the Secretary, acting through the Director, shall submit to Congress a report on the use of grants awarded under this section and any progress made toward the following:

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

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

''(B) Developing, implementing, or revising Cybersecurity Plans.

''(C) Reducing cybersecurity risks and cybersecurity threats to information systems, applications, and user accounts owned or operated by or on behalf of State, local, and Tribal organizations as a result of the award of such grants.

''(q) AUTHORIZATION OF APPROPRIATIONS.—There are authorized to be appropriated for grants under this section—

''(1) for each of fiscal years 2022 through 2026, $500,000,000; and

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

''SEC. 2220B. CYBERSECURITY RESOURCE GUIDE DEVELOPMENT FOR STATE, LOCAL, TRIBAL, AND TERRITORIAL GOVERNMENT OFFICIALS.

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

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

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

''Sec. 2220A. State and Local Cybersecurity Grant Program.
''Sec. 2220B. Cybersecurity resource guide development for State, local, Tribal, and territorial government officials.''.

SEC. 5423. STRATEGY.

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

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

''(1) IN GENERAL.—

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

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

''(B) RECOMMENDATIONS AND REQUIREMENTS.—The strategy required under subparagraph (A) shall—

''(i) provide recommendations relating to the ways in which the Federal Government should support and promote the ability of State, local, Tribal, and territorial governments to identify, mitigate against, protect against, detect, respond to, and recover from cybersecurity risks (as such term is defined in section 2209), cybersecurity threats, and incidents (as such term is defined in section 2209); and

''(ii) establish baseline requirements for cybersecurity plans under this section and principles with which such plans shall align.

''(2) CONTENTS.—The strategy required under paragraph (1) shall—

''(A) identify capability gaps in the ability of State, local, Tribal, and territorial governments to identify, protect against, detect, respond to, and recover from cybersecurity risks, cybersecurity threats, incidents, and ransomware incidents;

''(B) identify Federal resources and capabilities that are available or could be made available to State, local, Tribal, and territorial governments to help those governments identify, protect against, detect, respond to, and recover from cybersecurity risks, cybersecurity threats, incidents, and ransomware incidents;

''(C) identify and assess the limitations of Federal resources and capabilities available to State, local, Tribal, and territorial governments to help those governments identify, protect against, detect, respond to, and recover from cybersecurity risks, cybersecurity threats, incidents, and ransomware incidents and make recommendations to address such limitations;

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

Information Sharing and Analysis Center, to improve—

''(i) incident exercises, information sharing and incident notification procedures;

''(ii) the ability for State, local, Tribal, and territorial governments to voluntarily adapt and implement guidance in Federal binding operational directives; and

''(iii) opportunities to leverage Federal schedules for cybersecurity investments under section 502 of title 40, United States Code;

''(E) recommend new initiatives the Federal Government should undertake to improve the ability of State, local, Tribal, and territorial governments to identify, protect against, detect, respond to, and recover from cybersecurity risks, cybersecurity threats, incidents, and ransomware incidents;

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

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

''(G) set dates, including interim benchmarks, as appropriate for State, local, Tribal, and territorial governments to establish baseline capabilities to identify, protect against, detect, respond to, and recover from cybersecurity risks, cybersecurity threats, incidents, and ransomware incidents.

''(3) CONSIDERATIONS.—In developing the strategy required under paragraph (1), the Director, in coordination with the heads of appropriate Federal agencies, State, local, Tribal, and territorial governments, the State and Local Cybersecurity Resilience Committee established under section 2220A, and other stakeholders, as appropriate, shall consider—

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

''(B) the impact of incidents that have affected State, local, Tribal, and territorial governments, including the resulting costs to such governments;

''(C) the information related to the interest and ability of state and non-state threat actors to compromise information systems (as such term is defined in section 102 of the Cybersecurity Act of 2015 (6 U.S.C. 1501)) owned or operated by State, local, Tribal, and territorial governments;

''(D) emerging cybersecurity risks and cybersecurity threats to State, local, Tribal, and territorial governments resulting from the deployment of new technologies; and

''(E) recommendations made by the State and Local Cybersecurity Resilience Committee established under section 2220A.

''(4) EXEMPTION.—Chapter 35 of title 44, United States Code (commonly known as the 'Paperwork Reduction Act'), shall not apply to any action to implement this subsection.''.

(b) RESPONSIBILITIES OF THE DIRECTOR OF THE CYBERSECURITY AND INFRASTRUCTURE SECURITY AGENCY.—Section 2202 of the Homeland Security Act of 2002 (6 U.S.C. 652) is amended—

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

(2) by inserting after subsection (c) the following new subsection:

''(d) ADDITIONAL RESPONSIBILITIES.—In addition to the responsibilities under subsection (c), the Director shall—

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

''(2) review, in consultation with the State and Local Cybersecurity Resilience Committee, all cybersecurity plans of State, local, Tribal, and territorial governments developed pursuant to any homeland security assistance administered by the Department to improve cybersecurity;

''(3) provide expertise and technical assistance to State, local, Tribal, and territorial government officials with respect to cybersecurity; and

''(4) provide education, training, and capacity development to enhance the security and resilience of cybersecurity and infrastructure security.''.

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

SEC. 5424. CYBERSECURITY VULNERABILITIES.

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

(1) in subsection (a)—

(A) by redesignating paragraphs (4) through (8) as paragraphs (5) through (9), respectively; and

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

''(4) the term 'cybersecurity vulnerability' has the meaning given the term 'security vulnerability' in section 102 of the Cybersecurity Information Sharing Act of 2015 (6 U.S.C. 1501);''.

(2) in subsection (c)—

(A) in paragraph (5)—

(i) in subparagraph (A), by striking ''and'' after the semicolon at the end;

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

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

''(B) sharing mitigation protocols to counter cybersecurity vulnerabilities pursuant to subsection (n); and''; and

(iv) in subparagraph (C), as so redesignated, by inserting ''and mitigation protocols to counter cybersecurity vulnerabilities in accordance with subparagraph (B)'' before ''with Federal'';

(B) in paragraph (7)(C), by striking ''sharing'' and inserting ''share''; and

(C) in paragraph (9), by inserting ''mitigation protocols to counter cybersecurity vulnerabilities,'' after ''measures,'';

(3) in subsection (e)(1)(G), by striking the semicolon after ''and'' at the end;

(4) by redesignating subsection (o) as subsection (p); and

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

''(o) PROTOCOLS TO COUNTER CERTAIN CYBERSECURITY VULNERABILITIES.—The Director may, as appro-

priate, identify, develop, and disseminate actionable protocols to mitigate cybersecurity vulnerabilities to information systems and industrial control systems, including in circumstances in which such vulnerabilities exist because software or hardware is no longer supported by a vendor.''.

SEC. 5425. CAPABILITIES OF THE CYBERSECURITY AND INFRASTRUCTURE SECURITY AGENCY TO IDENTIFY THREATS TO INDUSTRIAL CONTROL SYSTEMS.

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

(1) in subsection (e)(1)—

(A) in subparagraph (G), by striking ''and;'' after the semicolon;

(B) in subparagraph (H), by inserting ''and'' after the semicolon; and

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

''(I) activities of the Center address the security of both information technology and operational technology, including industrial control systems;''; and

(2) by adding at the end the following new subsection:

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

''(1) lead Federal Government efforts, in consultation with Sector Risk Management Agencies, as appropriate, to identify and mitigate cybersecurity threats to industrial control systems, including supervisory control and data acquisition systems;

''(2) maintain threat hunting and incident response capabilities to respond to industrial control system cybersecurity risks and incidents;

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

''(4) collect, coordinate, and provide vulnerability information to the industrial control systems community by, as appropriate, working closely with security researchers, industry end-users, product manufacturers, Sector Risk Management Agencies,

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

''(5) conduct such other efforts and assistance as the Secretary determines appropriate.''.

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

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

cludes findings and recommendations relating to such implementation. Such report shall include information on the following:

(1) Any interagency coordination challenges to the ability of the Director of the Cybersecurity and Infrastructure Agency of the Department of Homeland Security to lead Federal efforts to identify and mitigate cybersecurity threats to industrial control systems pursuant to subsection (p)(1) of such section.

(2) The degree to which the Agency has adequate capacity, expertise, and resources to carry out threat hunting and incident response capabilities to mitigate cybersecurity threats to industrial control systems pursuant to subsection (p)(2) of such section, as well as additional resources that would be needed to close any operational gaps in such capabilities.

(3) The extent to which industrial control system stakeholders sought cybersecurity technical assistance from the Agency pursuant to subsection (p)(3) of such section, and the utility and effectiveness of such technical assistance.

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

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

SEC. 5426. REPORT ON CYBERSECURITY VULNERABILITIES.

(a) REPORT.—Not later than 1 year after the date of the enactment of this Act, the Director of the Cybersecurity and Infrastructure Security Agency of the Department of Homeland Security shall submit to the Committee on Homeland Security of the House of Representatives and the Committee on Homeland Security and Governmental Affairs of the Senate a report on how the Agency carries out subsection (n) of section 2209 of the Homeland Security Act of 2002 to coordinate vulnerability disclosures, including disclosures of cybersecurity vulnerabilities (as such term is defined in such section), and subsection (o) of such section (as added by section 5324) to disseminate actionable protocols to mitigate cybersecurity vulnerabilities to information systems and industrial control systems, that include the following:

(1) A description of the policies and procedures relating to the coordination of vulnerability disclosures.

(2) A description of the levels of activity in furtherance of such subsections (n) and (o) of such section 2209.

(3) Any plans to make further improvements to how information provided pursuant to such subsections can be shared (as such term is defined in such section 2209) between the Department and industry and other stakeholders.

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

(5) A description of how privacy and civil liberties are preserved in the collection, retention, use, and sharing of vulnerability disclosures.

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

SEC. 5427. COMPETITION RELATING TO CYBERSECURITY VULNERABILITIES.

The Under Secretary for Science and Technology of the Department of Homeland Security, in consultation with the Director of the Cybersecurity and Infrastructure Security Agency of the Department, may establish an incentive-based program that allows industry, individuals, academia, and others to compete in identifying remediation solutions for cybersecurity vulnerabilities (as such term is defined in section 2209 of the Homeland Security Act of 2002, as amended by section 5325) to information

systems (as such term is defined in such section 2209) and industrial control systems, including supervisory control and data acquisition systems.

SEC. 5428. NATIONAL CYBER EXERCISE PROGRAM.

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

"SEC. 2220C. NATIONAL CYBER EXERCISE PROGRAM.

''(a) ESTABLISHMENT OF PROGRAM.—

''(1) IN GENERAL.—There is established in the Agency the National Cyber Exercise Program (referred to in this section as the 'Exercise Program') to evaluate the National Cyber Incident Response Plan, and other related plans and strategies.

''(2) REQUIREMENTS.—

''(A) IN GENERAL.—The Exercise Program shall be—

''(i) based on current risk assessments, including credible threats, vulnerabilities, and consequences;

''(ii) designed, to the extent practicable, to simulate the partial or complete incapacitation of a government or critical

infrastructure network resulting from a cyber incident;

''(iii) designed to provide for the systematic evaluation of cyber readiness and enhance operational understanding of the cyber incident response system and relevant information-sharing agreements; and

''(iv) designed to promptly develop after-action reports and plans that can quickly incorporate lessons learned into future operations.

''(B) MODEL EXERCISE SELECTION.—The Exercise Program shall—

''(i) include a selection of model exercises that government and private entities can readily adapt for use; and

''(ii) aid such governments and private entities with the design, implementation, and evaluation of exercises that—

''(I) conform to the requirements described in subparagraph (A);

''(II) are consistent with any applicable national, State, local, or Tribal strategy or plan; and

''(III) provide for systematic evaluation of readiness.

''(3) CONSULTATION.—In carrying out the Exercise Program, the Director may consult with appropriate representatives from Sector Risk Management Agencies, cybersecurity research stakeholders, and Sector Coordinating Councils.

''(b) DEFINITIONS.—In this section:

''(1) STATE.—The term 'State' means any State of the United States, the District of Columbia, the Commonwealth of Puerto Rico, the Northern Mariana Islands, the United States Virgin Islands, Guam, American Samoa, and any other territory or possession of the United States.

''(2) PRIVATE ENTITY.—The term 'private entity' has the meaning given such term in section 102 of the Cybersecurity Information Sharing Act of 2015 (6 U.S.C. 1501).''.

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

''Sec. 2220C. National Cyber Exercise Program.''.

Subtitle C—Transportation Security

SEC. 5431. SURVEY OF THE TRANSPORTATION SECURITY ADMINISTRATION WORKFORCE REGARDING COVID–19 RESPONSE.

(a) SURVEY.—Not later than 1 year after the date of the enactment of this Act, the Administrator of the Transportation Security Administration (referred to in this section as the ''Administrator''), in consultation with the labor organization certified as the exclusive representative of full- and part-time nonsupervisory Administration personnel carrying out screening functions under section 44901 of title 49, United States Code, shall conduct a survey of the Transportation Security Administration (referred to in this section as the ''Administration'') workforce regarding the Administration's response to the COVID–19 pandemic. Such survey shall be conducted in a manner that allows for the greatest practicable level of workforce participation.

(b) CONTENTS.—In conducting the survey required under subsection (a), the Administrator shall solicit feedback on the following:

(1) The Administration's communication and collaboration with the Administration's workforce regarding the Administration's response to the

COVID–19 pandemic and efforts to mitigate and monitor transmission of COVID–19 among its workforce, including through—

(A) providing employees with personal protective equipment and mandating its use;

(B) modifying screening procedures and Administration operations to reduce transmission among officers and passengers and ensuring compliance with such changes;

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

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

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

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

(c) REPORT.—Not later than 30 days after completing the survey required under subsection (a), the Administration shall provide a report summarizing the results of the survey to the Committee on Homeland Secu-

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

SEC. 5432. TRANSPORTATION SECURITY PREPAREDNESS PLAN.

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

''(x) TRANSPORTATION SECURITY PREPAREDNESS PLAN.—

''(1) IN GENERAL.—Not later than two years after the date of the enactment of this subsection, the Secretary of Homeland Security, acting through the Administrator, in coordination with the Chief Medical Officer of the Department of Homeland Security and in consultation with the partners identified under paragraphs (3)(A)(i) through (3)(A)(iv), shall develop a transportation security preparedness plan to address the event of a communicable disease outbreak. The Secretary, acting through the Administrator, shall ensure such plan aligns with relevant Federal plans and strategies for communicable disease outbreaks.

''(2) CONSIDERATIONS.—In developing the plan required under paragraph (1), the Secretary, acting

through the Administrator, shall consider each of the following:

''(A) The findings of the survey required under section 5331 of the National Defense Authorization Act for Fiscal Year 2022.

''(B) All relevant reports and recommendations regarding the Administration's response to the COVID–19 pandemic, including any reports and recommendations issued by the Comptroller General and the Inspector General of the Department of Homeland Security.

''(C) Lessons learned from Federal interagency efforts during the COVID–19 pandemic.

''(3) CONTENTS OF PLAN.—The plan developed under paragraph (1) shall include each of the following:

''(A) Plans for communicating and collaborating in the event of a communicable disease outbreak with the following partners:

''(i) Appropriate Federal departments and agencies, including the Department of Health and Human Services, the Centers for Disease Control and Prevention, the Department of Transportation, the De-

partment of Labor, and appropriate interagency task forces.

''(ii) The workforce of the Administration, including through the labor organization certified as the exclusive representative of full- and part-time non-supervisory Administration personnel carrying out screening functions under section 44901 of this title.

''(iii) International partners, including the International Civil Aviation Organization and foreign governments, airports, and air carriers.

''(iv) Public and private stakeholders, as such term is defined under subsection (t)(1)(C).

''(v) The traveling public.

''(B) Plans for protecting the safety of the Transportation Security Administration workforce, including—

''(i) reducing the risk of communicable disease transmission at screening checkpoints and within the Administration's workforce related to the Administra-

tion's transportation security operations and mission;

''(ii) ensuring the safety and hygiene of screening checkpoints and other workstations;

''(iii) supporting equitable and appropriate access to relevant vaccines, prescriptions, and other medical care; and

''(iv) tracking rates of employee illness, recovery, and death.

''(C) Criteria for determining the conditions that may warrant the integration of additional actions in the aviation screening system in response to the communicable disease outbreak and a range of potential roles and responsibilities that align with such conditions.

''(D) Contingency plans for temporarily adjusting checkpoint operations to provide for passenger and employee safety while maintaining security during the communicable disease outbreak.

''(E) Provisions setting forth criteria for establishing an interagency task force or other standing engagement platform with other appropriate Federal departments and agencies, in-

cluding the Department of Health and Human Services and the Department of Transportation, to address such communicable disease outbreak.

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

''(G) Considerations for assessing the appropriateness of issuing security directives and emergency amendments to regulated parties in various modes of transportation, including surface transportation, and plans for ensuring compliance with such measures.

''(H) A description of any potential obstacles, including funding constraints and limitations to authorities, that could restrict the ability of the Administration to respond appropriately to a communicable disease outbreak.

''(4) DISSEMINATION.—Upon development of the plan required under paragraph (1), the Administrator shall disseminate the plan to the partners identified under paragraph (3)(A) and to the Committee on Homeland Security of the House of Representatives and the Committee on Commerce, Science, and Transportation of the Senate.

''(5) REVIEW OF PLAN.—Not later than two years after the date on which the plan is disseminated under paragraph (4), and biennially thereafter, the Secretary, acting through the Administrator and in coordination with the Chief Medical Officer of the Department of Homeland Security, shall review the plan and, after consultation with the partners identified under paragraphs (3)(A)(i) through (3)(A)(iv), update the plan as appropriate.''.

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

(1) whether such plan aligns with relevant Federal plans and strategies for communicable disease outbreaks; and

(2) the extent to which the Transportation Security Administration is prepared to implement the plan.

SEC. 5433. AUTHORIZATION OF TRANSPORTATION SECURITY ADMINISTRATION PERSONNEL DETAILS.

(a) COORDINATION.—Pursuant to sections 106(m) and 114(m) of title 49, United States Code, the Administrator of the Transportation Security Administration may provide Transportation Security Administration personnel, who are not engaged in front line transportation security efforts, to other components of the Department and other Federal agencies to improve coordination with such components and agencies to prepare for, protect against, and respond to public health threats to the transportation security system of the United States.

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

SEC. 5434. TRANSPORTATION SECURITY ADMINISTRATION PREPAREDNESS.

(a) ANALYSIS.—

(1) IN GENERAL.—The Administrator of the Transportation Security Administration shall conduct an analysis of preparedness of the transportation security system of the United States for public health threats. Such analysis shall assess, at a minimum, the following:

(A) The risks of public health threats to the transportation security system of the United States, including to transportation hubs, transportation security stakeholders, Transportation Security Administration (TSA) personnel, and passengers.

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

(C) Impacts to TSA policies and procedures for securing the transportation security system.

(2) COORDINATION.—The analysis conducted of the risks described in paragraph (1)(A) shall be conducted in coordination with the Chief Medical Officer of the Department of Homeland Security, the

Secretary of Health and Human Services, and transportation security stakeholders.

(b) BRIEFING.—Not later than 180 days after the date of the enactment of this Act, the Administrator shall brief the appropriate congressional committees on the following:

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

(2) Technologies necessary to combat public health threats at security screening checkpoints to better protect from future public health threats TSA personnel, passengers, aviation workers, and other personnel authorized to access the sterile area of an airport through such checkpoints, and the estimated cost of technology investments needed to fully implement across the aviation system solutions to such threats.

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

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

information with relevant domestic and international entities during a public health threat to the transportation security system, and how TSA can improve its leadership role in such areas.

(c) DEFINITIONS.—In this section:

(1) The term ''appropriate congressional committees'' means—

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

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

(2) The term ''sterile area'' has the meaning given such term in section 1540.5 of title 49, Code of Federal Regulations.

(3) The term ''TSA'' means the Transportation Security Administration.

SEC. 5435. PLAN TO REDUCE THE SPREAD OF CORONAVIRUS AT PASSENGER SCREENING CHECKPOINTS.

(a) IN GENERAL.—Not later than 90 days after the date of the enactment of this Act, the Administrator, in coordination with the Chief Medical Officer of the Department of Homeland Security, and in consultation with the

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

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

(1) An identification of best practices developed in response to the coronavirus among foreign governments, airports, and air carriers conducting aviation security screening operations, as well as among Federal agencies conducting similar security screening operations outside of airports, including in locations where the spread of the coronavirus has been successfully contained, that could be further integrated into the United States aviation security system.

(2) Specific operational changes to aviation security screening operations informed by the identification of best practices under paragraph (1) that could be implemented without degrading aviation security and a corresponding timeline and costs for implementing such changes.

(c) CONSIDERATIONS.—In carrying out the identification of best practices under subsection (b), the Administrator shall take into consideration the following:

(1) Aviation security screening procedures and practices in place at security screening locations, including procedures and practices implemented in response to the coronavirus.

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

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

(4) The feasibility and effectiveness of implementing similar procedures and practices in locations where such are not already in place.

(5) The feasibility and potential benefits to security, public health, and travel facilitation of continuing any procedures and practices implemented in response to the COVID–19 national emergency beyond the end of such emergency.

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

supervisory TSA personnel carrying out screening functions under section 44901 of title 49, United States Code.

(e) SUBMISSION.—Upon issuance of the plan required under subsection (a), the Administrator shall submit the plan to the Committee on Homeland Security of the House of Representatives and the Committee on Commerce, Science, and Transportation of the Senate.

(f) ISSUANCE AND IMPLEMENTATION.—The Administrator shall not be required to issue or implement, as the case may be, the plan required under subsection (a) upon the termination of the COVID–19 national emergency except to the extent the Administrator determines such issuance or implementation, as the case may be, to be feasible and beneficial to security screening operations.

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

(h) DEFINITIONS.—In this section:

(1) The term ''Administrator'' means the Administrator of the Transportation Security Administration.

(2) The term ''coronavirus'' has the meaning given such term in section 506 of the Coronavirus Preparedness and Response Supplemental Appropriations Act, 2020 (Public Law 116–123).

(3) The term ''COVID–19 national emergency'' means the national emergency declared by the President under the National Emergencies Act (50 U.S.C. 1601 et seq.) on March 13, 2020, with respect to the coronavirus.

(4) The term ''public and private stakeholders'' has the meaning given such term in section 114(t)(1)(C) of title 49, United States Code.

(5) The term ''TSA'' means the Transportation Security Administration.

SEC. 5436. COMPTROLLER GENERAL REVIEW OF DEPARTMENT OF HOMELAND SECURITY TRUSTED TRAVELER PROGRAMS.

Not later than one year after the date of the enactment of this Act, the Comptroller General of the United States shall conduct a review of Department of Homeland Security trusted traveler programs. Such review shall examine the following:

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

(2) Whether the Department coordinates with the heads of other relevant Federal, State, local, Tribal, or territorial entities regarding redress procedures for disqualifying offenses not covered by the Department's own redress processes but which offenses impact an individual's enrollment in a trusted traveler program.

(3) How the Department may improve individuals' access to reconsideration procedures regarding a disqualifying offense for enrollment in a trusted traveler program that requires the involvement of any other Federal, State, local, Tribal, or territorial entity.

(4) The extent to which travelers are informed about reconsideration procedures regarding enrollment in a trusted traveler program.

SEC. 5437. ENROLLMENT REDRESS WITH RESPECT TO DEPARTMENT OF HOMELAND SECURITY TRUSTED TRAVELER PROGRAMS.

Notwithstanding any other provision of law, the Secretary of Homeland Security shall, with respect to an individual whose enrollment in a trusted traveler program was revoked in error extend by an amount of time equal to the period of revocation the period of active enrollment in such a program upon reenrollment in such a program by such an individual.

SEC. 5438. THREAT INFORMATION SHARING.

(a) PRIORITIZATION.—The Secretary of Homeland Security shall prioritize the assignment of officers and intelligence analysts under section 210A of the Homeland Security Act of 2002 (6 U.S.C. 124h) from the Transportation Security Administration and, as appropriate, from the Office of Intelligence and Analysis of the Department of Homeland Security, to locations with participating State, local, and regional fusion centers in jurisdictions with a high-risk surface transportation asset in order to enhance the security of such assets, including by improving timely sharing, in a manner consistent with the protection of privacy rights, civil rights, and civil liberties, of information regarding threats of terrorism and other threats, including targeted violence.

(b) INTELLIGENCE PRODUCTS.—Officers and intelligence analysts assigned to locations with participating State, local, and regional fusion centers under this section shall participate in the generation and dissemination of transportation security intelligence products, with an emphasis on such products that relate to threats of terrorism and other threats, including targeted violence, to surface transportation assets that—

(1) assist State, local, and Tribal law enforcement agencies in deploying their resources, including personnel, most efficiently to help detect, prevent, investigate, apprehend, and respond to such threats;

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

(3) enhance the Department of Homeland Security's situational awareness of such threats.

(c) CLEARANCES.—The Secretary of Homeland Security shall make available to appropriate owners and operators of surface transportation assets, and to any other person that the Secretary determines appropriate to foster greater sharing of classified information relating to threats of terrorism and other threats, including targeted violence, to surface transportation assets, the process of application for security clearances under Executive Order

No. 13549 (75 Fed. Reg. 162; relating to a classified national security information program) or any successor Executive order.

(d) GAO REPORT.—Not later than 2 years after the date of the enactment of this Act, the Comptroller General of the United States shall submit to the Committee on Homeland Security of the House of Representatives and the Committee on Homeland Security and Governmental Affairs of the Senate a review of the implementation of this section, together with any recommendations to improve information sharing with State, local, Tribal, territorial, and private sector entities to prevent, identify, and respond to threats of terrorism and other threats, including targeted violence, to surface transportation assets.

(e) DEFINITIONS.—In this section:

(1) The term ''surface transportation asset'' includes facilities, equipment, or systems used to provide transportation services by—

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

(B) a railroad carrier (as such term is defined in section 20102(3) of title 49, United States Code);

(C) an owner or operator of—

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

(ii) a bus terminal; or

(D) other transportation facilities, equipment, or systems, as determined by the Secretary.

(2) The term ''targeted violence'' means an incident of violence in which an attacker selected a particular target in order to inflict mass injury or death with no discernable political or ideological motivation beyond mass injury or death.

(3) The term ''terrorism'' means the terms—

(A) domestic terrorism (as such term is defined in section 2331(5) of title 18, United States Code); and

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

SEC. 5439. LOCAL LAW ENFORCEMENT SECURITY TRAINING.

(a) IN GENERAL.—The Secretary of Homeland Security, in consultation with public and private sector stakeholders, may in a manner consistent with the protection of privacy rights, civil rights, and civil liberties, develop, through the Federal Law Enforcement Training Centers, a training program to enhance the protection, preparedness, and response capabilities of law enforcement agencies with respect to threats of terrorism and other threats, including targeted violence, at a surface transportation asset.

(b) REQUIREMENTS.—If the Secretary of Homeland Security develops the training program described in subsection (a), such training program shall—

(1) be informed by current information regarding tactics used by terrorists and others engaging in targeted violence;

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

(3) prioritize training officers from law enforcement agencies that are eligible for or receive grants under sections 2003 or 2004 of the Homeland Security Act of 2002 (6 U.S.C. 604 and 605) and officers employed by railroad carriers that operate passenger service, including interstate passenger service.

(c) DEFINITIONS.—In this section:

(1) The term ''public and private sector stakeholders'' has the meaning given such term in section 114(u)(1)(c) of title 49, United States Code.

(2) The term ''surface transportation asset'' includes facilities, equipment, or systems used to provide transportation services by—

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

(B) a railroad carrier (as such term is defined in section 20102(3) of title 49, United States Code);

(C) an owner or operator of—

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

tion 1501(4) of the Implementing Recommendations of the 9/11 Commission Act of 2007 (Public Law 110–53; 6 U.S.C. 1151(4))); or

(ii) a bus terminal; or

(D) other transportation facilities, equipment, or systems, as determined by the Secretary.

(3) The term ''targeted violence'' means an incident of violence in which an attacker selected a particular target in order to inflict mass injury or death with no discernable political or ideological motivation beyond mass injury or death.

(4) The term ''terrorism'' means the terms—

(A) domestic terrorism (as such term is defined in section 2331(5) of title 18, United States Code); and

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

SEC. 5440. ALLOWABLE USES OF FUNDS FOR PUBLIC TRANSPORTATION SECURITY ASSISTANCE GRANTS.

Subparagraph (A) of section 1406(b)(2) of the Implementing Recommendations of the 9/11 Commission Act of

2007 (6 U.S.C. 1135(b)(2); Public Law 110–53) is amended by inserting ''and associated backfill'' after ''security training''.

SEC. 5441. PERIODS OF PERFORMANCE FOR PUBLIC TRANSPORTATION SECURITY ASSISTANCE GRANTS.

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

(1) by redesignating subsection (m) as subsection (n); and

(2) by inserting after subsection (l) the following new subsection:

''(m) PERIODS OF PERFORMANCE.—

''(1) IN GENERAL.—Except as provided in paragraph (2), funds provided pursuant to a grant awarded under this section for a use specified in subsection (b) shall remain available for use by a grant recipient for a period of not fewer than 36 months.

''(2) EXCEPTION.—Funds provided pursuant to a grant awarded under this section for a use specified in subparagraph (M) or (N) of subsection (b)(1) shall remain available for use by a grant recipient for a period of not fewer than 55 months.''.

SEC. 5442. GAO REVIEW OF PUBLIC TRANSPORTATION SECURITY ASSISTANCE GRANT PROGRAM.

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

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

(1) An assessment of the type of projects funded under the public transportation security grant program referred to in such paragraph.

(2) An assessment of the manner in which such projects address threats to public transportation infrastructure.

(3) An assessment of the impact, if any, of sections 5342 through 5345 (including the amendments made by this Act) on types of projects funded under the public transportation security assistance grant program.

(4) An assessment of the management and administration of public transportation security assistance grant program funds by grantees.

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

program funds address vulnerabilities in public transportation infrastructure.

(6) Recommendations to improve the management and administration of the public transportation security assistance grant program.

(c) REPORT.—Not later than one year after the date of the enactment of this Act and again not later than five years after such date of enactment, the Comptroller General of the United States shall submit to the Committee on Homeland Security of the House of Representatives and the Committee on Homeland Security and Governmental Affairs of the Senate a report on the review required under this section.

SEC. 5443. SENSITIVE SECURITY INFORMATION; INTERNATIONAL AVIATION SECURITY.

(a) SENSITIVE SECURITY INFORMATION.—

(1) IN GENERAL.—Not later than 90 days after the date of the enactment of this Act, the Administrator of the Transportation Security Administration (TSA) shall—

(A) ensure clear and consistent designation of ''Sensitive Security Information'', including reasonable security justifications for such designation;

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

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

(D) document justifications for changes in position regarding Sensitive Security Information redactions and designations, and make such changes accessible to TSA personnel for use with relevant stakeholders, including air carriers, airport operators, surface transportation operators, and State and local law enforcement, as necessary; and

(E) ensure that TSA personnel are adequately trained on appropriate designation policies.

(2) STAKEHOLDER OUTREACH.—Not later than 180 days after the date of the enactment of this Act, the Administrator of the Transportation Security Administration (TSA) shall conduct outreach to relevant stakeholders described in paragraph (1)(D) that regularly are granted access to Sensitive Security Information to raise awareness of the TSA's

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

(b) INTERNATIONAL AVIATION SECURITY.—

(1) IN GENERAL.—Not later than 60 days after the date of the enactment of this Act, the Administrator of the Transportation Security Administration shall develop and implement guidelines with respect to last point of departure airports to—

(A) ensure the inclusion, as appropriate, of air carriers and other transportation security stakeholders in the development and implementation of security directives and emergency amendments;

(B) document input provided by air carriers and other transportation security stakeholders during the security directive and emergency amendment, development, and implementation processes;

(C) define a process, including timeframes, and with the inclusion of feedback from air carriers and other transportation security stakeholders, for cancelling or incorporating security directives and emergency amendments into security programs;

(D) conduct engagement with foreign partners on the implementation of security directives and emergency amendments, as appropriate, including recognition if existing security measures at a last point of departure airport are found to provide commensurate security as intended by potential new security directives and emergency amendments; and

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

(2) BRIEFING TO CONGRESS.—Not later than 90 days after the date of the enactment of this Act, the Administrator of the Transportation Security Administration shall brief the Committee on Homeland Security of the House of Representatives and the Committee on Commerce, Science, and Transportation of the Senate on the guidelines described in paragraph (1).

(3) DECISIONS NOT SUBJECT TO JUDICIAL REVIEW.—Notwithstanding any other provision of law, any action of the Administrator of the Transportation Security Administration under paragraph (1) is not subject to judicial review.

☒