(Original Signature of Member)

116TH CONGRESS
2D SESSION

H. R. _____

To authorize certain authorities of the Department of Homeland Security, and for other purposes.

IN THE HOUSE OF REPRESENTATIVES

Mr. ROGERS of Alabama introduced the following bill; which was referred to the Committee on _____

A BILL

To authorize certain authorities of the Department of Homeland Security, and for other purposes.

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

SECTION 1. SHORT TITLE; TABLE OF CONTENTS.

(a) SHORT TITLE.—This Act may be cited as the "Keep America Secure Act".

(b) TABLE OF CONTENTS.—The table of contents for this Act is as follows:

Sec. 1. Short title; table of contents.
Sec. 2. Authorization of appropriations.

TITLE I—MANAGEMENT REFORM AND ACCOUNTABILITY

Subtitle A—Headquarters Operation

Sec. 101. Homeland security enterprise defined.
Sec. 102. Functions and components of headquarters of Department of Homeland Security.
Sec. 103. Repeal of Director of Shared Services and Office of Counternarcotics Enforcement of Department of Homeland Security.
Sec. 104. Responsibilities and functions of Chief Privacy Officer.
Sec. 105. Unmanned Aircraft Systems Countermeasures Coordinator.
Sec. 106. Responsibilities of Chief Financial Officer.
Sec. 107. Chief Information Officer.
Sec. 108. Quadrennial homeland security review.
Sec. 109. Office of Strategy, Policy, and Plans.
Sec. 110. Chief Procurement Officer.
Sec. 111. Chief Security Officer.
Sec. 112. Office of Partnership and Engagement.
Sec. 113. Department of Homeland Security rotation program.
Sec. 114. Annual submission to Congress of information regarding reprogramming or transfer of Department of Homeland Security resources to respond to operational surges.
Sec. 115. Overseas personnel briefing.

Subtitle B—Acquisition Reform

Sec. 121. Acquisition Review Board.
Sec. 122. Acquisition authorities for Under Secretary for Management of the Department of Homeland Security.
Sec. 123. Acquisition authorities for Under Secretary of Strategy, Policy, and Plans.
Sec. 124. Acquisition authorities for Program Accountability and Risk Management (PARM).
Sec. 125. Government Accountability Office review of board and of requirements to reduce duplication in acquisition programs.
Sec. 126. Excluded party list system waivers.
Sec. 127. Inspector general oversight of suspension and debarment.
Sec. 128. Congressional notification for major acquisition programs.
Sec. 129. Multiyear acquisition strategy.
Sec. 130. Acquisition reports.
Sec. 131. Prohibition on operation or procurement of foreign-made unmanned aircraft systems.
Sec. 132. Establishment of the Office of Biometric Identity Management.

Subtitle C—Management of Programs

Sec. 141. Department of Homeland Security enhanced hiring.
Sec. 142. Fitness standards.
Sec. 143. Training to protect the vulnerable.
Sec. 144. Department of Homeland Security Blue Campaign enhancement.

TITLE II—INTELLIGENCE AND INFORMATION SHARING

Subtitle A—DHS Intelligence Enterprise

Sec. 201. Annual homeland threat assessments.
Sec. 202. Homeland intelligence doctrine.
Sec. 203. Comptroller General assessment.
Sec. 204. Analysts for the chief intelligence officer.

Sec. 205. Establishment of Insider Threat Program.
Sec. 206. Department of Homeland Security counterintelligence vetting task force.
Sec. 207. Visa security.
Sec. 208. Chemical, biological, radiological, and nuclear intelligence and information sharing.
Sec. 209. Inland waters threat analysis.
Sec. 210. Transnational criminal organizations threat assessment.
Sec. 211. Department of Homeland Security counterterrorism advisory board.
Sec. 212. National Vetting Center.
Sec. 213. National Vetting Governance Board.

Subtitle B—Information Sharing

Sec. 215. Department of Homeland Security Fusion Center Partnership Initiative.
Sec. 216. Fusion center personnel needs assessment.
Sec. 217. Program for State and local analyst clearances.
Sec. 218. Information technology assessment.
Sec. 219. Department of Homeland Security classified facility inventory and dissemination.
Sec. 220. Terror inmate information sharing.
Sec. 221. Enhancing Department of Homeland Security suspicious activity reporting operations.

TITLE III—CYBERSECURITY

Sec. 301. Cybersecurity Advisory Committee.
Sec. 302. Cybersecurity essentials.
Sec. 303. Establishment of continuous diagnostics and mitigation program in the Cybersecurity and Infrastructure Security Agency.
Sec. 304. Administrative subpoena authority.
Sec. 305. CISA Director term limitation.
Sec. 306. State, local, Tribal and terroritorial cybersecurity.
Sec. 307. Cybersecurity workforce.
Sec. 308. Election security.
Sec. 309. Protection from liability.
Sec. 310. Permanent extension of chemical facility anti-terrorism standards program of the Department of Homeland Security.
Sec. 311. Cybersecurity research and development projects.
Sec. 312. Loan repayment program.
Sec. 313. Exclusion of certain student loan repayments.
Sec. 314. Scholarship for service.
Sec. 315. Cybersecurity and Infrastructure Security Agency review.
Sec. 316. Strategy to secure email.
Sec. 317. Strengthening Federal networks.
Sec. 318. Authorization of appropriations.

TITLE IV—BORDER AND VISA SECURITY

Sec. 401. Additional U.S. Customs and Border Protection agents and officers.
Sec. 402. Establishment of workload staffing models for U.S. Border Patrol and Air and Marine Operations of CBP.
Sec. 403. U.S. Customs and Border Protection retention incentives.
Sec. 404. Study on efficacy of certain personnel screening methods for U.S. Customs and Border Protection use.

Sec. 405. Hiring flexibility.
Sec. 406. Supplemental commissioner authority and definitions.
Sec. 407. Technical and conforming amendment.
Sec. 408. Ports of entry infrastructure.
Sec. 409. U.S. Customs and Border Protection technology upgrades.
Sec. 410. Physical barriers along the southwest border.
Sec. 411. Air and Marine Operations flight hours.
Sec. 412. Amendments to U.S. Customs and Border Protection.
Sec. 413. Continuous screening by U.S. Customs and Border Protection.
Sec. 414. Customs Trade Partnership Against Terrorism.
Sec. 415. Strategy to ensure detection of all opioid purity levels at ports of entry.
Sec. 416. Authorization of the immigration advisory program.
Sec. 417. Border security technology accountability.
Sec. 418. Establishment of U.S. Immigration and Customs Enforcement.
Sec. 419. Biometric identification transnational migration alert program.
Sec. 420. Reporting of visa overstays.
Sec. 421. Student and exchange visitor information system verification.
Sec. 422. Social media review of visa applicants.
Sec. 423. Homeland security investigations national gang unit.
Sec. 424. Homeland security investigations transnational criminal investigative units.
Sec. 425. Homeland security investigations innovation lab.
Sec. 426. Establishment of United States Citizenship and Immigration Services.
Sec. 427. Fraud prevention.
Sec. 428. Border security and trade modernization trust fund.
Sec. 429. Border security improvement plan.
Sec. 430. Integrated Border Enforcement Teams.
Sec. 431. No ban on information sharing.
Sec. 432. Border Security advisory committee.
Sec. 433. Border tunnel detection.
Sec. 434. Subterranean operations.
Sec. 435. Border enforcement security task force updates.
Sec. 436. Extension of port of entry donation authority.

TITLE V—TRANSPORTATION SECURITY

Sec. 501. Authorization of appropriations for salaries, operation, and maintenance of the Transportation Security Administration.
Sec. 502. Retention of security service fee by the Transportation Security Administration.
Sec. 503. Emerging and future threats task force.
Sec. 504. Comptroller General review.
Sec. 505. Enrollment redress.
Sec. 506. Training required.
Sec. 507. Identity and travel document verification.
Sec. 508. Standard operating procedures at airport checkpoints.
Sec. 509. Canine detection research and development.
Sec. 510. Security incident response at airports and surface transportation hubs.
Sec. 511. Alternate new security screening personnel training program cost and feasibility study.
Sec. 512. Prohibition of advance notice of covert testing to security screeners.
Sec. 513. Explosive detection technology.

Sec. 514. Recurrent vetting for surface transportation credential-holders.
Sec. 515. Biometrics for TSA PreCheck.
Sec. 516. Secure Flight program.
Sec. 517. Known Crew Member program.
Sec. 518. Screening Partnership Program.
Sec. 519. Headquarters efficiency.
Sec. 520. Repeal of regulations.
Sec. 521. Sensitive security information.
Sec. 522. International aviation security.
Sec. 523. Office of Inspection accountability.
Sec. 524. Checkpoints of the future.
Sec. 525. Air cargo security.
Sec. 526. Childcare.
Sec. 527. Passengers with physical or cognitive disabilities.
Sec. 528. TSA Human Capital Strategic Plan.
Sec. 529. Screening technology deployment.
Sec. 530. Review of aviation security stakeholder access to Homeland Security Information Network.
Sec. 531. Airport public area security enhancement.

TITLE VI—EMERGENCY PREPAREDNESS, RESPONSE, AND RECOVERY

Subtitle A—Grants, Training, Exercises, and Coordination

Sec. 601. Urban Area Security Initiative.
Sec. 602. State Homeland Security Grant Program.
Sec. 603. Grants to directly eligible tribes.
Sec. 604. Law enforcement terrorism prevention.
Sec. 605. Prioritization.
Sec. 606. Allowable uses.
Sec. 607. Memoranda of understanding.
Sec. 608. Grants metrics.
Sec. 609. Grant management best practices.
Sec. 610. Prohibition on consolidation.
Sec. 611. Maintenance of grant investments.
Sec. 612. Allowable uses of funds for public transportation security assistance grants.
Sec. 613. Periods of performance for public transportation security assistance grants.
Sec. 614. Comptroller General review of public transportation security assistance grant program.
Sec. 615. Port security grant program.
Sec. 616. Cyber preparedness.
Sec. 617. Operation Stonegarden.

Subtitle B—Communications

Sec. 621. Office of Emergency Communications.
Sec. 622. Responsibilities of Office of Emergency Communications Director.
Sec. 623. Annual reporting on activities of the Office of Emergency Communications.
Sec. 624. National emergency communications plan.
Sec. 625. Technical edit.
Sec. 626. Public safety broadband network.
Sec. 627. Communications training.

Subtitle C—Federal Emergency Management Agency (FEMA)

Sec. 631. Short title.
Sec. 632. Reauthorization of Federal Emergency Management Agency.
Sec. 633. National domestic preparedness consortium.
Sec. 634. Rural Domestic Preparedness Consortium.
Sec. 635. Center for Faith-Based and Neighborhood Partnerships.
Sec. 636. Emergency support functions.
Sec. 637. Review of national incident management system.
Sec. 638. Remedial action management program.
Sec. 639. Strategic human capital plan.
Sec. 640. Office of Disability Integration and Coordination.
Sec. 641. FEMA Senior Law Enforcement Advisor.
Sec. 642. Technical amendments to national emergency management.

Subtitle D—Genome Editing Threat Assessment

Sec. 651. Genome editing threat assessment.

TITLE VII—PANDEMIC PREPAREDNESS

Sec. 701. Chief Medical Officer.
Sec. 702. Medical countermeasures program.
Sec. 703. Personal protective equipment.
Sec. 704. Teleworking assessment.
Sec. 705. Transportation security public health threat preparedness.
Sec. 706. Securing critical supplies.

SEC. 2. AUTHORIZATION OF APPROPRIATIONS.

There is authorized to be appropriated for the necessary expenses of the Department of Homeland Security authorized by this Act, the amendments made by this Act, and other provisions of law (including relevant provisions of title 49, United States Code, and the Homeland Security Act of 2002 (6 U.S.C. 101 et seq.))—

(1) $59,100,000,000 for fiscal year 2021, of which—

(A) $11,975,942,980 shall be for grants and agency expenditures as provided in titles III, IV, V, and VI and the amendments made by such titles; and

(B) $7,917,936,000 shall be for the Transportation Security Administration as provided by section 114(w) of title 49, United States Code; and

(2) $60,200,000,000 for fiscal year 2022, of which $20,477,721,840 shall be for grants and agency expenditures as provided in titles III, IV, V, and VI and the amendments made by such titles.

TITLE I—MANAGEMENT REFORM AND ACCOUNTABILITY

Subtitle A—Headquarters Operation

SEC. 101. HOMELAND SECURITY ENTERPRISE DEFINED.

Section 2 of the Homeland Security Act of 2002 (6 U.S.C. 101) is amended—

(1) by redesignating paragraphs (9) through (20) as paragraphs (10) through (21), respectively; and

(2) by inserting after paragraph (8) the following new paragraph (9):

''(9) The term 'homeland security enterprise' means any relevant governmental or nongovernmental entity involved in homeland security, including a Federal, State, or local government official,

private sector representative, academic, or other policy expert.''.

SEC. 102. FUNCTIONS AND COMPONENTS OF HEADQUARTERS OF DEPARTMENT OF HOMELAND SECURITY.

Section 102 of the Homeland Security Act of 2002 (6 U.S.C. 112) is amended—

(1) in subsection (b)—

(A) in paragraph (2), by striking ''and'' after the semicolon at the end;

(B) in paragraph (3), by striking the period and inserting ''; and''; and

(C) by adding at the end the following:

''(4) may enter into agreements with governments of other countries, in consultation with the Secretary of State and international nongovernmental organizations, in order to achieve the missions of the Department.''; and

(2) in subsection (c), in the matter preceding paragraph (1), by striking ''through the Office of State and Local Coordination (established under section 801)'' and inserting ''through the Office of Partnership and Engagement''; and

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

1 ''(h) HEADQUARTERS.—

2 ''(1) COMPONENTS.—There is in the Depart-
3 ment a Headquarters. The Department Head-
4 quarters shall include each of the following:

5 ''(A) The Office of the Secretary.

6 ''(B) The Office of the Deputy Secretary.

7 ''(C) The Executive Secretary.

8 ''(D) The Management Directorate, includ-
9 ing the Office of the Chief Financial Officer.

10 ''(E) The Science and Technology Direc-
11 torate.

12 ''(F) The Office of Strategy, Policy, and
13 Plans.

14 ''(G) The Office of the General Counsel.

15 ''(H) The Office of the Chief Privacy Offi-
16 cer.

17 ''(I) The Office for Civil Rights and Civil
18 Liberties.

19 ''(J) The Office of Operations Coordina-
20 tion.

21 ''(K) The Office of Intelligence and Anal-
22 ysis.

23 ''(L) The Office of Legislative Affairs.

24 ''(M) The Office of Public Affairs.

25 ''(N) The Office of the Inspector General.

"(O) The Office of the Citizenship and Immigration Services Ombudsman.

"(P) The Office of Partnership and Engagement.

"(Q) The Countering Weapons of Mass Destruction Office.

"(2) FUNCTIONS.—The Secretary, acting through the appropriate official of the Headquarters, shall—

"(A) establish an overall strategy to successfully further the mission of the Department;

"(B) establish initiatives that improve Department-wide operational performance;

"(C) establish mechanisms to—

"(i) ensure that components of the Department comply with Department policies and fully implement the strategies and initiatives of the Secretary; and

"(ii) require the head of each component of the Department and component chief officers to comply with such policies and implement such strategies and initiatives;

"(D) establish annual operational and management objectives to evaluate the performance of the Department;

"(E) ensure that the Department successfully meets operational and management performance objectives through conducting oversight of component agencies;

"(F) ensure that the strategies, priorities, investments, and workforce of Department components align with Department objectives;

"(G) establish and implement policies related to Department ethics and compliance standards;

"(H) establish and implement, in consultation with the Office of Civil Rights and Civil Liberties, policies which preserve individual liberty, fairness, and equality under the law;

"(I) manage and encourage shared services across Department components;

"(J) lead and coordinate interaction with Congress and other external organizations; and

"(K) carry out other such functions as the Secretary determines are appropriate.".

SEC. 103. REPEAL OF DIRECTOR OF SHARED SERVICES AND OFFICE OF COUNTERNARCOTICS ENFORCEMENT OF DEPARTMENT OF HOMELAND SECURITY.

(a) ABOLISHMENT OF DIRECTOR OF SHARED SERVICES.—

(1) ABOLISHMENT.—The position of Director of Shared Services of the Department of Homeland Security is abolished.

(2) CONFORMING AMENDMENT.—The Homeland Security Act of 2002 is amended by striking section 475 (6 U.S.C. 295).

(3) CLERICAL AMENDMENT.—The table of contents in section 1(b) of such Act is amended by striking the item relating to section 475.

(b) ABOLISHMENT OF THE OFFICE OF COUNTERNARCOTICS ENFORCEMENT.—

(1) ABOLISHMENT.—The Office of Counternarcotics Enforcement is abolished.

(2) CONFORMING AMENDMENTS.—The Homeland Security Act of 2002 is amended—

(A) in subparagraph (B) of section 843(b)(1) (6 U.S.C. 413(b)(1)), by striking ''by—'' and all that follows through the end of that subparagraph and inserting ''by the Secretary; and''; and

(B) by striking section 878 (6 U.S.C. 112).

(3) CLERICAL AMENDMENT.—The table of contents in section 1(b) of such Act is amended by striking the item relating to section 878.

SEC. 104. RESPONSIBILITIES AND FUNCTIONS OF CHIEF PRIVACY OFFICER.

(a) IN GENERAL.—Section 222 of the Homeland Security Act of 2002 (6 U.S.C. 142) is amended—

(1) in subsection (a)—

(A) in the matter preceding paragraph (1)—

(i) by inserting ''to be the Chief Privacy Officer of the Department and, if the Secretary so appoints, the Chief Freedom of Information Act (FOIA) Officer,'' after ''in the Department,''; and

(ii) by striking ''to the Secretary, to assume primary responsibility for privacy policy'' and inserting ''to the Secretary. Such official shall be deemed the equivalent of an Assistant Secretary, and shall assume primary responsibility for privacy policy and, if determined appropriate by

the Secretary, FOIA policy, of the Department''; (B) in paragraph (5)(B), by striking ''and'' at the end; and (C) by striking paragraph (6) and inserting the following new paragraphs:

''(6) developing guidance and recommendations to assist components of the Department in developing privacy policies and practices;

''(7) establishing a mechanism to ensure such components are in compliance with Federal, regulatory, statutory, and Department privacy requirements, mandates, directives, and policies;

''(8) working with the Chief Information Officer of the Department to identify methods for managing and overseeing the records, management policies, and procedures of the Department;

''(9) working with components and offices of the Department to ensure that policy development, information sharing, and information management activities incorporate disclosure considerations and privacy protections;

''(10) serving as the Chief FOIA Officer of the Department for purposes of subsection (j) of section 552 of title 5, United States Code (popularly known

as the Freedom of Information Act), to manage and process requests related to such section;

''(11) developing guidance on procedures to be followed by individuals making requests for information under such section 552;

''(12) overseeing hiring of FOIA officers and the management and processing of requests for information under such section 552 within Department Headquarters and relevant Department component offices;

''(13) identifying and eliminating unnecessary and duplicative technology and actions taken by the Department in the course of processing requests for information under such section 552;

''(14) preparing an annual report to Congress that includes a description of—

''(A) the activities of the Department that affect privacy during the fiscal year covered by the report, including complaints of privacy violations, implementation of section 552a of title 5, United States Code (popularly known as the Privacy Act of 1974), internal controls, and other matters; and

''(B) insignificant programs implemented or revised in the Department during the fiscal

year covered by the report, the number of programs that the Chief Privacy Officer has evaluated to ensure that privacy protections are considered and implemented, the number of programs reviewed that effectively implemented privacy protections, and an explanation of why any new programs did not effectively implement privacy protections;

''(15) issuing guidance to relevant Department component offices to ensure uniform disclosure policies and processes to administer such section 552; and

''(16) carrying out such other responsibilities as the Secretary determines are appropriate, consistent with this section.''; and

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

''(f) REASSIGNMENT OF FUNCTIONS.—Notwithstanding any requirement under this section, the Secretary may reassign the functions related to managing and processing requests for information under section 552 of title 5, United States Code, to another officer within the Department, consistent with requirements of such section.

''(g) WORKING GROUP.—

1 "(1) IN GENERAL.—The Chief Privacy Officer,
2 or, if the Secretary determines appropriate, whoever
3 is appointed by the Secretary as the Chief FOIA Of-
4 ficer, shall establish and serve as the Chair of a
5 working group comprised of personnel from across
6 the Department who are involved in executing disclo-
7 sure policies and processes involved in administra-
8 tion of section 552 of title 5, United States Code
9 (commonly referred to as the 'Freedom of Informa-
10 tion Act').
11 "(2) PURPOSE.—The working group established
12 in accordance with paragraph (1) shall be a forum—
13 "(A) for the sharing of information and
14 best practices; and
15 "(B) to develop solutions to challenges en-
16 countered within Department component offices
17 relating to disclosure policies and processes re-
18 ferred to in such paragraph.
19 "(3) RESPONSIBILITIES.—Members of the
20 working group shall meet not less than once every
21 quarter to advise the Chair on matters concerning
22 disclosure policies and processes involved in the ad-
23 ministration of section 552 of title 5, United States
24 Code, including on the following matters:

"(A) The development of guidance for uniform disclosure policies and processes, in accordance with paragraph (15) of subsection (a).

"(B) Ways to reduce unnecessary redundancies that may undermine the responsive and efficient processing of requests for information under such section 552.".

SEC. 105. UNMANNED AIRCRAFT SYSTEMS COUNTERMEASURES COORDINATOR.

(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. 321. COUNTERING UNMANNED AIRCRAFT SYSTEMS COORDINATOR.

"(a) COORDINATOR.—The Secretary shall designate a senior official of the Office of Strategy, Policy and Plans of the Department as the Countering Unmanned Aircraft Systems (UAS) Coordinator (in this section referred to as the 'Coordinator') to coordinate with relevant Department offices and components, including the Office for Civil Rights and Civil Liberties and the Privacy Office and other relevant Federal agencies, as appropriate, on the development of policies and plans to counter threats associated with UAS in accordance with section 210G, including the following:

"(1) Promoting research and development of counter UAS technologies, in coordination with the Office of Science and Technology of the Department.

"(2) Ensuring the dissemination of information and guidance related to countering UAS threats.

"(3) Coordinate with the relevant components and offices of the Department, including the Office of Intelligence and Analysis, to ensure the sharing and retention of information, guidance, and intelligence relating to countering UAS threats, counter UAS threat assessment, and counter UAS technology.

"(4) Serving as the Department point of contact for Federal, State, local, and Tribal law enforcement entities and the private sector regarding the Department's activities related to countering UAS.

"(5) Carrying out other related UAS authorities and activities under such section 210G, as directed by the Secretary.

"(b) COORDINATION WITH APPLICABLE FEDERAL LAWS.—The Coordinator shall, in addition to other assigned duties, coordinate with relevant Department offices and components and other relevant Federal agencies, as appropriate, to ensure testing, evaluation, or deployment

of a system used to identify, assess, or defeat a UAS is carried out in accordance with applicable Federal laws.

''(c) COORDINATION WITH PRIVATE SECTOR.—The Coordinator shall, working with the Office of Partnership and Engagement and other relevant Department offices and components, or other Federal agencies, as appropriate, serve as the principal Department official responsible for disseminating to the private sector information regarding counter UAS technology, particularly information regarding instances in which counter UAS technology may impact lawful private sector services or systems.

''(d) TERMINATION.—The authority to carry out this section terminates on the date specified in section 210G(i).''.

(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 320 the following new item:

''Sec. 321. Countering Unmanned Aircraft Systems Coordinator.''.

SEC. 106. RESPONSIBILITIES OF CHIEF FINANCIAL OFFICER.

(a) IN GENERAL.—Section 702 of the Homeland Security Act of 2002 (6 U.S.C. 342) is amended—

(1) by redesignating subsections (b) and (c) as subsections (c) and (d), respectively; and

(2) by inserting after subsection (a) the following new subsection (b):

"(b) RESPONSIBILITIES.—In carrying out the responsibilities, authorities, and functions specified in section 902 of title 31, United States Code, the Chief Financial Officer shall—

"(1) oversee Department budget formulation and execution;

"(2) lead and provide guidance on performance-based budgeting practices for the Department to ensure that the Department and its components are meeting missions and goals;

"(3) lead cost-estimating practices for the Department, including the development of policies on cost estimating and approval of life cycle cost estimates;

"(4) coordinate with the Office of Strategy, Policy, and Plans to ensure that the development of the budget for the Department is compatible with the long-term strategic plans, priorities, and policies of the Secretary;

"(5) develop financial management policy for the Department and oversee the implementation of such policy, including the establishment of effective

internal controls over financial reporting systems and processes throughout the Department;

''(6) provide guidance for and over financial system modernization efforts throughout the Department;

''(7) lead the efforts of the Department related to financial oversight, including identifying ways to streamline and standardize business processes;

''(8) oversee the costs of acquisition programs and related activities to ensure that actual and planned costs are in accordance with budget estimates and are affordable, or can be adequately funded, over the lifecycle of such programs and activities;

''(9) fully implement a common accounting structure to be used across the entire Department by fiscal year 2022; and

''(10) track, approve, oversee, and make public information on expenditures by components of the Department for conferences, as appropriate, including by requiring each component to—

''(A) report to the Inspector General of the Department the expenditures by such component for each conference hosted or attended by Department employees for which the total expenditures of the Department exceed $20,000,

within 15 days after the date of the conference; and

"(B) with respect to such expenditures, provide to the Inspector General—

"(i) the information described in subsections (a), (b), and (c) of section 739 of title VII of division E of the Consolidated and Further Continuing Appropriations Act, 2015 (Public Law 113-235); and

"(ii) documentation of such expenditures.".

(b) RULE OF CONSTRUCTION.—Nothing in the amendment made by this section may be construed as altering or amending the responsibilities, authorities, and functions of the Chief Financial Officer of the Department of Homeland Security under section 902 of title 31, United States Code.

SEC. 107. CHIEF INFORMATION OFFICER.

(a) IN GENERAL.—Section 703 of the Homeland Security Act of 2002 (6 U.S.C. 343) is amended—

(1) in subsection (a), by adding at the end the following new sentence: "In addition to the functions under section 3506(a)(2) of title 44, United States Code, the Chief Information Officer shall perform

the functions set forth in this section and such other functions as may be assigned by the Secretary.'';

(2) by redesignating subsection (b) as subsection (d); and

(3) by inserting after subsection (a) the following new subsections:

''(b) RESPONSIBILITIES.—In addition to performing the functions under section 3506 of title 44, United States Code, the Chief Information Officer shall serve as the lead technical authority for information technology programs of the Department and Department components, and shall—

''(1) advise and assist the Secretary, heads of the components of the Department, and other senior officers in carrying out the responsibilities of the Department for all activities relating to the budgets, programs, security, and operations of the information technology functions of the Department;

''(2) to the extent delegated by the Secretary, exercise leadership and authority over Department information technology management and establish the information technology priorities, policies, processes, standards, guidelines, and procedures of the Department to ensure interoperability and standardization of information technology;

1 ''(3) maintain a consolidated inventory of the
2 mission critical and mission essential information
3 systems of the Department, and develop and main-
4 tain contingency plans for responding to a disrup-
5 tion in the operation of any of those information sys-
6 tems;
7 ''(4) maintain the security, visibility, reliability,
8 integrity, and availability of data and information
9 technology of the Department;
10 ''(5) establish and implement policies and pro-
11 cedures to effectively monitor and manage
12 vulnerabilities in the supply chain for purchases of
13 information technology, in consultation with the
14 Chief Procurement Officer of the Department;
15 ''(6) review contracts and interagency agree-
16 ments associated with major information technology
17 investments and information technology investments
18 that have had cost, schedule, or performance chal-
19 lenges in the past;
20 ''(7) assess the risk of all major information
21 technology investments and publicly report the risk
22 rating to the Office of Management and Budget;
23 ''(8) oversee the management of the Homeland
24 Security Enterprise Architecture technology system
25 and ensure that, before each acquisition decision

1 event (as such term is defined in section 839), ap-
2 proved information technology acquisitions comply
3 with any departmental information technology man-
4 agement requirements, security protocols, and the
5 Homeland Security Enterprise Architecture, and in
6 any case in which information technology acquisi-
7 tions do not comply with the Department's manage-
8 ment directives, making recommendations to the De-
9 partment's Acquisition Review Board regarding such
10 noncompliance;
11 ''(9) provide recommendations to the Acquisi-
12 tion Review Board regarding information technology
13 programs, and developing information technology ac-
14 quisition strategic guidance; and
15 ''(10) carry out any other responsibilities dele-
16 gated by the Secretary consistent with an effective
17 information system management function.
18 ''(c) STRATEGIC PLANS.—In coordination with the
19 Chief Financial Officer, the Chief Information Officer
20 shall develop an information technology strategic plan
21 every five years and report to the Committee on Homeland
22 Security and the Committee on Appropriations of the
23 House of Representatives and the Committee on Home-
24 land Security and Governmental Affairs and the Com-

mittee on Appropriations of the Senate on the extent to which—

"(1) the budget of the Department aligns with priorities specified in the information technology strategic plan;

"(2) the information technology strategic plan informs the budget process of the Department;

"(3) information technology priorities were or were not funded and the reasons for not funding all priorities in a given fiscal year;

"(4) the Department has identified and addressed skills gaps needed to implement the information technology strategic plan; and

"(5) unnecessary duplicate information technology within and across the components of the Department has been eliminated.".

(b) SOFTWARE LICENSING.—

(1) SOFTWARE INVENTORY.—Not later than 180 days after the date of the enactment of this Act and every two years thereafter until 2024, the Chief Information Officer of the Department of Homeland Security, in consultation with Department component chief information officers, shall—

(A) conduct a Department-wide inventory of all existing software licenses held by the De-

1 partment, including utilized and unutilized li-
2 censes;
3 (B) assess the needs of the Department
4 and the components of the Department for soft-
5 ware licenses for the subsequent two fiscal
6 years;
7 (C) examine how the Department can
8 achieve the greatest possible economies of scale
9 and cost savings in the procurement of software
10 licenses;
11 (D) determine how the use of shared
12 cloud-computing services will impact the needs
13 for software licenses for the subsequent two fis-
14 cal years;
15 (E) establish plans and estimated costs for
16 eliminating unutilized software licenses for the
17 subsequent two fiscal years; and
18 (F) submit a copy of each inventory con-
19 ducted under subparagraph (A) to the Com-
20 mittee on Homeland Security of the House of
21 Representatives and the Committee on Home-
22 land Security and Governmental Affairs of the
23 Senate.
24 (2) PLAN TO REDUCE SOFTWARE LICENSES.—
25 If the Chief Information Officer determines through

the inventory conducted under paragraph (1) that the number of software licenses held by the Department and the components of the Department exceed the needs of the Department, not later than 90 days after the date on which the inventory is completed, the Secretary of Homeland Security shall establish a plan for reducing the number of such software licenses to meet needs of the Department.

(3) PROHIBITION ON PROCUREMENT OF NEW SOFTWARE LICENSES.—

(A) IN GENERAL.—Except as provided in subparagraph (B), upon completion of a plan under paragraph (2), no additional resources may be obligated for the procurement of new software licenses for the Department until such time as the need of the Department exceeds the number of used and unused licenses held by the Department.

(B) EXCEPTION.—The Chief Information Officer may authorize the purchase of additional licenses and amend the number of needed licenses as necessary.

(c) COMPTROLLER GENERAL REVIEW.—Not later than fiscal year 2022, the Comptroller General of the United States shall review the extent to which the Chief

Information Officer fulfilled all requirements established in this section and the amendment made by this section.

(d) COMPLETION OF FIRST DEFINITION OF CAPABILITIES.—Not later than one year after the date of the enactment of this Act, the Chief Information Officer shall complete the first information technology strategic plan required under subsection (c) of section 701 of the Homeland Security Act of 2002, as added by subsection (a) of this section.

SEC. 108. 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'' at the end;

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

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

''(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 '', including any resources identified from redundant, wasteful, or unnecessary capabilities and capacities that can be redirected to better sup-

port other existing capabilities and 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 submittal 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);

(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 covered by the 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, 2020.

SEC. 109. OFFICE OF STRATEGY, POLICY, AND PLANS.

(a) IN GENERAL.—Section 709 of the Homeland Security Act of 2002 (6 U.S.C. 349) is amended—

(1) in subsection (a), by adding at the end he following: ''The Office of Strategy, Policy, and Plans shall include the following components:

''(1) The Office of International Affairs.

''(2) The Office of Cyber Policy.

''(3) The Office of Strategy, Planning, Analysis, and Risk.

''(4) The Office of Threat Prevention and Security Policy.

''(5) The Office of Border, Immigration, and Trade Policy.''.

(2) by redesignating subsections (e) through (g) as subsections (f) through (h), respectively; and

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

"(e) ASSISTANT SECRETARY FOR INTERNATIONAL AFFAIRS.—The Office of International Affairs shall be led by an Assistant Secretary for International Affairs appointed by the Secretary. The Assistant Secretary shall—

"(1) coordinate international activities within the Department, including activities carried out by the components of the Department, in consultation with other Federal officials with responsibility for counterterrorism and homeland security matters;

"(2) advise, inform, and assist the Secretary with respect to the development and implementation of the policy priorities of the Department, including strategic priorities for the deployment of assets, including personnel, outside the United States;

"(3) develop, in consultation with the Under Secretary for Management, guidance for selecting, assigning, training, and monitoring overseas deployments of Department personnel, including minimum standards for pre-deployment training;

"(4) maintain awareness regarding the international travel of senior officers of the Department and their intent to pursue negotiations with foreign

government officials, and review resulting draft agreements; and

''(5) perform such other functions as are established by law or delegated by the Under Secretary for Policy.''.

(b) ABOLISHMENT OF OFFICE OF INTERNATIONAL AFFAIRS.—

(1) IN GENERAL.—The Office of International Affairs within the Office of the Secretary of Homeland Security is abolished.

(2) TRANSFER OF ASSETS AND PERSONNEL.—The functions authorized to be performed by such office as of the day before the date of the enactment of this Act, and the assets and personnel associated with such functions, are transferred to the head of the Office of International Affairs provided for by section 709 of the Homeland Security Act of 2002, as amended by this section.

(3) CONFORMING AMENDMENT.—The Homeland Security Act of 2002 is amended by striking section 879 (6 U.S.C. 459).

(4) CLERICAL AMENDMENT.—The table of contents in section 1(b) of such Act is amended by striking the item relating to section 879.

(c) CONFORMING AMENDMENTS RELATING TO ASSISTANT SECRETARIES.—Subsection (a) of section 103 of the Homeland Security Act of 2002 (6 U.S.C. 113) is amended—

(1) in the subsection heading, by inserting "; Assistant Secretaries and Other Officers" after "Under Secretaries";

(2) in paragraph (1), by amending subparagraph (I) to read as follows:

"(I) An Administrator of the Transportation Security Administration.";

(3) by amending paragraph (2) to read as follows:

"(2) ASSISTANT SECRETARIES.—The following Assistant Secretaries shall be appointed by the President or the Secretary, as the case may be, without the advice and consent of the Senate:

"(A) PRESIDENTIAL APPOINTMENTS.—The Department shall have the following officials appointed by the President:

"(i) The Assistant Secretary for the Countering Weapons of Mass Destruction Office.

"(ii) The Assistant Secretary for Public Affairs.

1 "(iii) The Assistant Secretary for
2 Legislative Affairs.
3 "(iv) The Chief Medical Officer.
4 "(B) SECRETARIAL APPOINTMENTS.—The
5 Department shall have the following Assistant
6 Secretaries appointed by the Secretary:
7 "(i) The Principal Assistant Secretary
8 for External Affairs.
9 "(ii) The Assistant Secretary, Office
10 of Cybersecurity and Communications.
11 "(iii) The Assistant Secretary for
12 International Affairs.
13 "(iv) The Assistant Secretary for
14 Partnership and Engagement.
15 "(v) The Assistant Secretary for
16 Threat Prevention and Security Policy.
17 "(vi) The Assistant Secretary for Bor-
18 der, Immigration, and Trade Policy.
19 "(vii) The Assistant Secretary for
20 Cyber, Infrastructure, and Resilience Pol-
21 icy.
22 "(viii) The Assistant Secretary for
23 Strategy, Planning, Analysis, and Risk.
24 "(ix) The Assistant Secretary for
25 State and Local Law Enforcement."; and

(4) by adding at the end the following new paragraph:

''(3) ASSISTANT SECRETARY FOR LEGISLATIVE AFFAIRS.—The Assistant Secretary for Legislative Affairs shall oversee one internal reporting structure for engaging with authorizing and appropriating congressional committees.''.

(d) HOMELAND SECURITY ADVISORY COUNCIL.—Subsection (b) of section 102 of the Homeland Security Act of 2002 (6 U.S.C. 112) is amended—

(1) in paragraph (2), by striking ''and'' at the end;

(2) in paragraph (3), by striking the period at the end and inserting ''; and''; and

(3) by adding at the end the following new paragraph:

''(4) shall establish a Homeland Security Advisory Council to provide advice and recommendations on homeland security-related matters, including advice with respect to the preparation of the Quadrennial Homeland Security Review.''.

(e) DEFINITIONS.—In this section each of the terms ''functions'', ''assets'', and ''personnel'' has the meaning given each such term under section 2 of the Homeland Security Act of 2002 (6 U.S.C. 101).

(f) DUPLICATION REVIEW.—

(1) REVIEW REQUIRED.—Not later than one year after the date of the enactment of this Act, the Secretary of Homeland Security shall complete a review of the functions and responsibilities of each Department of Homeland Security component responsible for international affairs to identify and eliminate areas of unnecessary duplication.

(2) SUBMISSION TO CONGRESS.—Not later than 60 days after the completion of the review required under paragraph (1), the Secretary shall provide the results of the review to the Committee on Homeland Security of the House of Representatives and the Committee on Homeland Security and Governmental Affairs of the Senate.

(3) ACTION PLAN.—Not later than one year after the date of the enactment of this Act, the Secretary shall submit to the congressional homeland security committees an action plan, including corrective steps and an estimated date of completion, to address areas of duplication, fragmentation, and overlap and opportunities for cost savings and revenue enhancement, as identified by the Government Accountability Office based on the annual report of the Government Accountability Office entitled ''Ad-

ditional Opportunities to Reduce Fragmentation, Overlap, and Duplication and Achieve Other Financial Benefits''.

SEC. 110. CHIEF PROCUREMENT OFFICER.

(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. CHIEF PROCUREMENT OFFICER.

''(a) IN GENERAL.—There is in the Department a Chief Procurement Officer, who shall serve as a senior business advisor to agency officials on procurement-related matters and report directly to the Under Secretary for Management. The Chief Procurement Officer is the senior procurement executive for purposes of subsection (c) of section 1702 of title 41, United States Code, and shall perform procurement functions as specified in such subsection.

''(b) RESPONSIBILITIES.—The Chief Procurement Officer shall—

''(1) delegate or retain contracting authority, as appropriate;

''(2) issue procurement policies and oversee the heads of contracting activity of the Department to ensure compliance with those policies;

1 ''(3) serve as the main liaison of the Depart-
2 ment to industry on procurement-related issues;
3 ''(4) account for the integrity, performance, and
4 oversight of Department procurement and con-
5 tracting functions;
6 ''(5) ensure that procurement contracting strat-
7 egies and plans are consistent with the intent and
8 direction of the Acquisition Review Board;
9 ''(6) oversee a centralized acquisition workforce
10 certification and training program using, as appro-
11 priate, existing best practices and acquisition train-
12 ing opportunities from the Federal Government, pri-
13 vate sector, or universities and colleges to include
14 training on how best to identify actions that warrant
15 referrals for suspension or debarment;
16 ''(7) provide input on the periodic performance
17 reviews of each head of contracting activity of the
18 Department;
19 ''(8) collect baseline data and use such data to
20 establish performance measures on the impact of
21 strategic sourcing initiatives on the private sector,
22 including small businesses;
23 ''(9) establish and implement policies and pro-
24 cedures to effectively monitor and manage

vulnerabilities in the supply chain for all Department purchases;

''(10) ensure that a fair proportion of the value of Federal contracts and subcontracts are awarded to small businesses (in accordance with the procurement contract goals under section 15(g) of the Small Business Act (15 U.S.C. 644(g)), maximize opportunities for small business participation in such contracts, and ensure, to the extent practicable, small businesses that achieve qualified vendor status for security-related technologies are provided an opportunity to compete for contracts for such technology;

''(11) conduct oversight of implementation of administrative agreements to resolve suspension or debarment proceedings; and

''(12) carry out any other procurement duties that the Under Secretary for Management may designate.

''(c) HEAD OF CONTRACTING ACTIVITY DEFINED.—In this section the term 'head of contracting activity' means an official responsible for the creation, management, and oversight of a team of procurement professionals properly trained, certified, and warranted to accomplish the acquisition of products and services on behalf of the designated components, offices, and organizations

of the Department, and as authorized, other government entities.''.

(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. Chief Procurement Officer.''.

SEC. 111. CHIEF SECURITY OFFICER.

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

''SEC. 712. CHIEF SECURITY OFFICER.

''(a) IN GENERAL.—There is in the Department a Chief Security Officer, who shall report directly to the Under Secretary for Management.

''(b) RESPONSIBILITIES.—The Chief Security Officer shall—

''(1) develop and implement the security policies, programs, and standards of the Department;

''(2) identify training and provide education to Department personnel on security-related matters; and

''(3) provide support to Department components on security-related matters.''.

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

"Sec. 712. Chief Security Officer.".

SEC. 112. OFFICE OF PARTNERSHIP AND ENGAGEMENT.

(a) IN GENERAL.—Section 801 of the Homeland Security Act of 2002 (6 U.S.C. 361) is amended to read as follows:

"SEC. 801. OFFICE OF PARTNERSHIP AND ENGAGEMENT.

"(a) ESTABLISHMENT.—There is established within the Office of the Secretary an Office of Partnership and Engagement, which shall be led by an Assistant Secretary.

"(b) RESPONSIBILITIES.—The Assistant Secretary shall—

"(1) lead the efforts of the Department to incorporate external feedback from stakeholders into policy and strategic planning efforts, as appropriate, in consultation with the Office for Civil Rights and Civil Liberties;

"(2) oversee and support the activities conducted under section 2006(b);

"(3) advise the Secretary on the effects of the policies, regulations, processes, and actions of the Department on the private sector and create and foster strategic communications with the private sec-

tor to enhance the primary mission of the Department to protect the homeland;

''(4) coordinate the activities of the Department relating to State and local governments;

''(5) provide State and local governments with regular information, research, and technical support to assist State and local efforts at securing the homeland; and

''(6) perform such other functions as are established by law or delegated by the Secretary.''.

(b) OFFICE FOR STATE AND LOCAL LAW ENFORCEMENT.—Paragraph (1) of section 2006(b) of the Homeland Security Act of 2002 (6 U.S.C. 607(b)) is amended by striking ''Policy Directorate'' and inserting ''Office of Partnership and Engagement''.

(c) ABOLISHMENT OF OFFICE FOR STATE AND LOCAL GOVERNMENT COORDINATION.—

(1) IN GENERAL.—The Office for State and Local Government Coordination of the Department of Homeland Security is abolished.

(2) TRANSFER OF FUNCTIONS AND ASSETS.—The functions authorized to be performed by such office as of the day before the date of the enactment of this Act, and the assets and personnel associated with such functions, are transferred to the head of

Office of Partnership and Engagement under section 801 of the Homeland Security Act of 2002, as amended by this section.

(d) ABOLISHMENT OF SPECIAL ASSISTANT TO SECRETARY OF HOMELAND SECURITY.—

(1) IN GENERAL.—The position of Special Assistant to the Secretary of Homeland Security authorized under section 102(f) of the Homeland Security Act of 2002 (6 U.S.C. 112(f)), as in effect on the day before the date of the enactment of this Act, is abolished.

(2) TRANSFER OF FUNCTIONS AND ASSETS.—The functions authorized to be performed by such Special Assistant to the Secretary as of the day before such date of enactment, and the assets and personnel associated with such functions, are transferred to the head of the Office of Partnership and Engagement under section 801 of the Homeland Security Act of 2002, as amended by this section.

(3) CONFORMING AMENDMENT.—Section 102 of the Homeland Security Act of 2002 (6 U.S.C. 112) is amended by—

(A) striking subsection (f); and

(B) redesignating subsection (g) as subsection (f).

(e) CLERICAL AMENDMENT.—The table of contents in section 1(b) of such Act is amended by amending the item relating to section 801 to read as follows:

"Sec. 801. Office of Partnership and Engagement.".

SEC. 113. DEPARTMENT OF HOMELAND SECURITY ROTATION PROGRAM.

(a) ENHANCEMENTS TO THE ROTATION PROGRAM.—Section 844 of the Homeland Security Act of 2002 (6 U.S.C. 414) is amended—

(1) by striking "(a) ESTABLISHMENT—.";

(2) by redesignating paragraphs (1) through (5) as subsections (a) through (e), respectively, and adjusting the margins accordingly;

(3) in subsection (a), as so redesignated—

(A) by striking "Not later than 180 days after the date of enactment of this section, the" and inserting "The"; and

(B) by striking "for employees of the Department" and inserting "for certain personnel within the Department";

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

(A) by redesignating subparagraphs (A) through (G) as paragraphs (3) through (9), respectively, and adjusting the margins accordingly;

(B) by inserting before paragraph (3), as so redesignated, the following new paragraphs:

''(1) seek to foster greater departmental integration and unity of effort;

''(2) seek to help enhance the knowledge, skills, and abilities of participating personnel with respect to the programs, policies, and activities of the Department;'';

(C) in paragraph (4), as so redesignated, by striking ''middle and senior level''; and

(D) in paragraph (7), as so redesignated, by inserting before ''invigorate'' the following: ''seek to improve morale and retention throughout the Department and'';

(5) in subsection (c), as redesignated by paragraph (2)—

(A) by redesignating subparagraphs (A) and (B) as paragraphs (1) and (2), respectively, and adjusting the margins accordingly; and

(B) in paragraph (2), as so redesignated—

(i) by striking clause (iii); and

(ii) by redesignating clauses (i), (ii), and (iv) through (viii) as subparagraphs (A) through (G), respectively, and adjusting the margins accordingly;

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

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

''(d) ADMINISTRATIVE MATTERS.—In carrying out the Rotation Program the Secretary shall—

''(1) before selecting employees for participation in the Rotation Program, disseminate information broadly within the Department about the availability of the Rotation Program, qualifications for participation in the Rotation Program, including full-time employment within the employing component or office not less than one year, and the general provisions of the Rotation Program;

''(2) require as a condition of participation in the Rotation Program that an employee—

''(A) is nominated by the head of the component or office employing the employee; and

''(B) is selected by the Secretary, or the Secretary's designee, solely on the basis of relative ability, knowledge, and skills, after fair and open competition that assures that all candidates receive equal opportunity;

"(3) ensure that each employee participating in the Rotation Program shall be entitled to return, within a reasonable period of time after the end of the period of participation, to the position held by the employee, or a corresponding or higher position, in the component or office that employed the employee prior to the participation of the employee in the Rotation Program;

"(4) require that the rights that would be available to the employee if the employee were detailed from the employing component or office to another Federal agency or office remain available to the employee during the employee participation in the Rotation Program; and

"(5) require that, during the period of participation by an employee in the Rotation Program, performance evaluations for the employee—

"(A) shall be conducted by officials in the office or component employing the employee with input from the supervisors of the employee at the component or office in which the employee is placed during that period; and

"(B) shall be provided the same weight with respect to promotions and other rewards as performance evaluations for service in the of-

fice or component employing the employee.''; and

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

''(g) INTELLIGENCE ROTATIONAL ASSIGNMENT PROGRAM.—

''(1) ESTABLISHMENT.—The Secretary shall establish an Intelligence Rotational Assignment Program as part of the Rotation Program under subsection (a).

''(2) ADMINISTRATION.—The Chief Human Capital Officer, in conjunction with the Chief Intelligence Officer, shall administer the Intelligence Rotational Assignment Program established pursuant to paragraph (1).

''(3) ELIGIBLITY.—The Intelligence Rotational Assignment Program established pursuant to paragraph (1) shall be open to employees serving in existing analyst positions within the Department's Intelligence Enterprise and other Department employees as determined appropriate by the Chief Human Capital Officer and the Chief Intelligence Officer.

''(4) COORDINATION.—The responsibilities specified in subsection (c)(2) that apply to the Rotation Program under such subsection shall, as appli-

cable, also apply to the Intelligence Rotational Assignment Program under this subsection.''.

(b) CONGRESSIONAL NOTIFICATION AND OVERSIGHT.—Not later than 120 days after the date of the enactment of this Act, the Secretary of Homeland Security shall provide to the Committee on Homeland Security and the Permanent Select Committee on Intelligence of the House of Representatives and the Committee on Homeland Security and Governmental Affairs of the Senate information about the status of the Homeland Security Rotation Program authorized by section 844 of the Homeland Security Act of 2002, as amended by subsection (a) of this section.

SEC. 114. ANNUAL SUBMISSION TO CONGRESS OF INFORMATION REGARDING REPROGRAMMING OR TRANSFER OF DEPARTMENT OF HOMELAND SECURITY RESOURCES TO RESPOND TO OPERATIONAL SURGES.

(a) IN GENERAL.—Title VII of the Homeland Security Act of 2002, as amended by this title, is further amended by adding at the end the following new section:

"SEC. 713. ANNUAL SUBMISSION TO CONGRESS OF INFORMATION ON REPROGRAMMING OR TRANSFERS OF FUNDS TO RESPOND TO OPERATIONAL SURGES.

''For each fiscal year until fiscal year 2023, the Secretary 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, together with the annual budget request for the Department, information on—

''(1) any circumstance during the year covered by the report in which the Secretary exercised the authority to reprogram or transfer funds to address unforeseen costs, including costs associated with operational surges; and

''(2) any circumstance in which any limitation on the transfer or reprogramming of funds affected the ability of the Secretary to address such unforeseen costs.''.

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

''Sec. 713. Annual submission to Congress of information on reprogramming or transfers of funds to respond to operational surges.''.

SEC. 115. OVERSEAS PERSONNEL BRIEFING.

(a) BRIEFING REQUIRED.—

(1) IN GENERAL.—Not later than 90 days after the date of the enactment of this Act and every 180 days thereafter, the Secretary 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 regarding Department of Homeland Security personnel with primary duties that take place outside of the United States.

(2) REQUIREMENTS.—The briefings required under paragraph (1) shall include the following:

(A) A detailed summary of, and deployment schedule for, each type of personnel position with primary duties that take place outside of the United States and how each such position contributes to the Department of Homeland Security's counterterrorism mission.

(B) Information related to how the geographic and regional placement of such positions contributes to the Department's counterterrorism mission.

(C) Information related to any risk mitigation plans for each geographic and regional

1 placement, including to address counter-intel-
2 ligence risks.
3 (D) Information regarding the costs of de-
4 ploying or maintaining personnel at each geo-
5 graphic and regional placement, including infor-
6 mation on any cost-sharing agreement with for-
7 eign partners to cover a portion or all the costs
8 relating to such deployment or maintenance.
9 (E) Maintain and enhance practices to
10 guard against counter-espionage and counter-
11 intelligence threats, including cyber threats, as-
12 sociated with Department personnel.
13 (F) Information regarding trends in for-
14 eign efforts to influence such personnel while
15 deployed overseas to contribute to the Depart-
16 ment's counterterrorism mission.
17 (G) Information related to the position-
18 specific training received by such personnel be-
19 fore and during placement at a foreign location.
20 (H) Challenges that may impede the com-
21 munication of counterterrorism information be-
22 tween Department personnel at foreign loca-
23 tions and Department entities in the United
24 States, including technical, resource, and ad-
25 ministrative challenges.

(I) The status of efforts to implement the strategy referred to in paragraph (1).

(J) The status of efforts (beginning with the second briefing required under this subsection) to implement the enhancement plan under subsection (b).

(3) TERMINATION.—The briefing requirement under paragraph (1) shall terminate on the date that is 4 years after the submission of the strategy referred to in such paragraph.

(b) OVERSEAS PERSONNEL ENHANCEMENT PLAN.—

(1) IN GENERAL.—Not later than 90 days after the first briefing required under subsection (a), the Secretary shall submit to the Committee on Homeland Security of the House and the Committee on Homeland Security and Governmental Affairs of the Senate a plan to enhance the effectiveness of Department of Homeland Security personnel at foreign locations.

(2) PLAN REQUIREMENTS.—The plan required under paragraph (1) shall include proposals to—

(A) improve efforts of Department of Homeland Security personnel at foreign locations, as necessary, for purposes of providing foreign partner capacity development and fur-

thering the Department's counterterrorism mission;

(B) as appropriate, redeploy Department personnel to respond to changing threats to the United States;

(C) enhance collaboration among Department personnel at foreign locations, other Federal personnel at foreign locations, and foreign partners;

(D) improve the communication of counterterrorism information between Department personnel at foreign locations and Department entities in the United States, including to address technical, resource, and administrative challenges; and

(E) maintain practices to guard against counter-espionage threats associated with Department personnel.

Subtitle B—Acquisition Reform

SEC. 121. ACQUISITION REVIEW BOARD.

(a) IN GENERAL.—Subtitle D of title VIII of the Homeland Security Act of 2002 (6 U.S.C. 391 et seq.) is amended by adding at the end the following new section:

"SEC. 836. ACQUISITION REVIEW BOARD.

"(a) IN GENERAL.—The Secretary shall establish an Acquisition Review Board (in this section referred to as the 'Board') to—

"(1) strengthen accountability and uniformity within the Department acquisition review process;

"(2) review major acquisition programs; and

"(3) review the use of best practices.

"(b) COMPOSITION.—

"(1) CHAIR.—The Under Secretary for Management shall serve as chair of the Board.

"(2) PARTICIPATION.— The Secretary shall ensure participation by other relevant Department officials with responsibilities related to acquisitions as permanent members of the Board.

"(3) OVERSIGHT.—The Under Secretary for Management shall designate a full time employee of the Department to oversee the operations of the Board.

"(c) MEETINGS.—The Board shall meet regularly for purposes of ensuring all acquisitions processes proceed in a timely fashion to achieve mission readiness. The Board shall convene at the Secretary's discretion and at any time—

"(1) a major acquisition program—

"(A) requires authorization to proceed from one acquisition decision event to another throughout the acquisition life cycle;

"(B) is in breach of its approved requirements; or

"(C) requires additional review, as determined by the Under Secretary for Management; or

"(2) a non-major acquisition program requires review, as determined by the Under Secretary for Management.

"(d) RESPONSIBILITIES.—The responsibilities of the Board are as follows:

"(1) Determine whether a proposed acquisition has met the requirements of key phases of the acquisition life cycle framework and is able to proceed to the next phase and eventual full production and deployment.

"(2) Oversee whether a proposed acquisition's business strategy, resources, management, and accountability is executable and is aligned to strategic initiatives.

"(3) Support the person with acquisition decision authority for an acquisition in determining the

appropriate direction for such acquisition at key acquisition decision events.

''(4) Conduct systematic reviews of acquisitions to ensure that such acquisitions are progressing in compliance with the approved documents for their current acquisition phases.

''(5) Review the acquisition documents of each major acquisition program, including the acquisition program baseline and documentation reflecting consideration of tradeoffs among cost, schedule, and performance objectives, to ensure the reliability of underlying data.

''(6) Ensure that practices are adopted and implemented to require consideration of trade-offs among cost, schedule, and performance objectives as part of the process for developing requirements for major acquisition programs prior to the initiation of the second acquisition decision event, including, at a minimum, the following practices:

''(A) Department officials responsible for acquisition, budget, and cost estimating functions are provided with the appropriate opportunity to develop estimates and raise cost and schedule matters before performance objectives are established for capabilities when feasible.

"(B) Full consideration is given to possible trade-offs among cost, schedule, and performance objectives for each alternative.

"(e) ACQUISITION PROGRAM BASELINE REPORT REQUIREMENT.—If the person exercising acquisition decision authority over a major acquisition program approves such program to proceed into the planning phase before such program has a Department-approved acquisition program baseline, the Under Secretary for Management shall create and approve an acquisition program baseline report regarding such approval, and the Secretary shall—

"(1) within 7 days after an acquisition decision memorandum is signed, notify in writing the Committee on Homeland Security of the House of Representatives and the Committee on Homeland Security and Governmental Affairs of the Senate of such decision; and

"(2) within 60 days after the acquisition decision memorandum is signed, submit to such committees a written explanation of the rationale for such decision and a plan of action to address acquisition program baseline requirements for such program.

"(f) REPORT.—The Under Secretary for Management shall provide information to the Committee on Homeland Security of the House of Representatives and

the Committee on Homeland Security and Governmental Affairs of the Senate on an annual basis through fiscal year 2024 on the activities of the Board for the prior fiscal year that includes information relating to the following:

"(1) For each meeting of the Board, any acquisition decision memoranda.

"(2) Results of the systematic reviews conducted pursuant to paragraph (4) of subsection (d).

"(3) Results of acquisition document reviews required pursuant to paragraph (5) of subsection (d).

"(4) Activities to ensure that practices are adopted and implemented throughout the Department pursuant to paragraph (6) of subsection (d).

"(g) DEFINITIONS.—In this section:

"(1) ACQUISITION.—The term 'acquisition' has the meaning given such term in section 131 of title 41, United States Code.

"(2) ACQUISITION DECISION AUTHORITY.—The term 'acquisition decision authority' means the authority, held by the Secretary acting through the Deputy Secretary or Under Secretary for Management to—

"(A) ensure compliance with Federal law, the Federal Acquisition Regulation, and Department acquisition management directives;

"(B) review (including approving, pausing, modifying, or cancelling) an acquisition program through the life cycle of such program;

"(C) ensure that acquisition program managers have the resources necessary to successfully execute an approved acquisition program;

"(D) ensure good acquisition program management of cost, schedule, risk, and system performance of the acquisition program at issue, including assessing acquisition program baseline breaches and directing any corrective action for such breaches; and

"(E) ensure that acquisition program managers, on an ongoing basis, monitor cost, schedule, and performance against established baselines and use tools to assess risks to an acquisition program at all phases of the life cycle of such program to avoid and mitigate acquisition program baseline breaches.

"(3) ACQUISITION DECISION EVENT.—The term 'acquisition decision event', with respect to an acquisition program, means a predetermined point within each of the acquisition phases at which the acquisition decision authority determines whether such ac-

quisition program shall proceed to the next acquisition phase.

''(4) ACQUISITION DECISION MEMORANDUM.—The term 'acquisition decision memorandum', with respect to an acquisition, means the official acquisition decision event record that includes a documented record of decisions, exit criteria, and assigned actions for such acquisition, as determined by the person exercising acquisition decision authority for such acquisition.

''(5) ACQUISITION PROGRAM.—The term 'acquisition program' means the process by which the Department acquires, with any appropriated amounts, by contract for purchase or lease, property or services (including construction) that support the missions and goals of the Department.

''(6) ACQUISITION PROGRAM BASELINE.—The term 'acquisition program baseline', with respect to an acquisition program, means a summary of the cost, schedule, and performance parameters, expressed in standard, measurable, quantitative terms, which must be met in order to accomplish the goals of such program.

''(7) BEST PRACTICES.—The term 'best practices', with respect to acquisition, means a knowl-

edge-based approach to capability development that includes—

"(A) identifying and validating needs;

"(B) assessing alternatives to select the most appropriate solution;

"(C) clearly establishing well-defined requirements;

"(D) developing realistic cost assessments and schedules;

"(E) securing stable funding that matches resources to requirements;

"(F) demonstrating technology, design, and manufacturing maturity;

"(G) using milestones and exit criteria or specific accomplishments that demonstrate progress;

"(H) adopting and executing standardized processes with known success across programs;

"(I) establishing an adequate workforce that is qualified and sufficient to perform necessary functions; and

"(J) integrating the capabilities described in subparagraphs (A) through (I) into the Department's mission and business operations.

"(8) MAJOR ACQUISITION PROGRAM.—The term 'major acquisition program' means a Department acquisition program that is estimated by the Secretary to require an eventual total expenditure of at least $300 million (based on fiscal year 2019 constant dollars) over its life cycle cost.".

(b) CLERICAL AMENDMENT.—The table of contents in section 1(b) of the Homeland Security Act of 2002 (6 U.S.C. 101 et seq.) is amended by inserting after the item relating to section 835 the following new item:

"Sec. 836. Acquisition Review Board.".

SEC. 122. ACQUISITION AUTHORITIES FOR UNDER SECRETARY FOR MANAGEMENT OF THE DEPARTMENT OF HOMELAND SECURITY.

Section 701 of the Homeland Security Act of 2002 (6 U.S.C. 341) is amended by—

(1) redesignating subsection (d), the first subsection (e) (relating to the system for award management consultation), and the second subsection (e) (relating to the definition of interoperable communications) as subsections (e), (f), and (g), respectively; and

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

"(d) ACQUISITION AND RELATED RESPONSIBILITIES.—

"(1) IN GENERAL.—Notwithstanding section 1702(a) of title 41, United States Code, the Under Secretary for Management is the Chief Acquisition Officer of the Department. As Chief Acquisition Officer, the Under Secretary shall have the authorities and perform the functions specified in such section 1702(b), and perform all other functions and responsibilities delegated by the Secretary or described in this subsection.

"(2) FUNCTIONS AND RESPONSIBILITIES.—In addition to the authorities and functions specified in section 1702(b) of title 41, United States Code, the functions and responsibilities of the Under Secretary for Management related to acquisition (as such term is defined in section 836) include the following:

"(A) Advising the Secretary regarding acquisition management activities, taking into account risks of failure to achieve cost, schedule, or performance parameters, to ensure that the Department achieves its mission through the adoption of widely accepted program management best practices (as such term is defined in section 836) and standards and, where appropriate, acquisition innovation best practices.

"(B) Leading the Department's acquisition oversight body, the Acquisition Review Board.

"(C) Exercising the acquisition decision authority (as such term is defined in section 836) to approve, pause, modify (including the rescission of approvals of program milestones), or cancel major acquisition programs (as such term is defined in section 836), unless the Under Secretary delegates such authority to a Component Acquisition Executive (as such term is defined in section 836) pursuant to paragraph (3).

"(D) Establishing policies for acquisition that implement an approach that takes into account risks of failure to achieve cost, schedule, or performance parameters that all components of the Department shall comply with, including outlining relevant authorities for program managers to effectively manage acquisition programs (as such term is defined in section 836).

"(E) Ensuring that each major acquisition program has a Department-approved acquisition program baseline (as such term is defined in section 836), pursuant to the Department's acquisition management policy.

"(F) Assisting the heads of components and Component Acquisition Executives in efforts to comply with Federal law, the Federal Acquisition Regulation, and Department acquisition management directives.

"(G) Ensuring that grants and financial assistance are provided only to individuals and organizations that are not suspended or debarred.

"(H) Distributing guidance throughout the Department to ensure that contractors involved in acquisitions, particularly contractors that access the Department's information systems and technologies, adhere to relevant Department policies related to physical and information security as identified by the Under Secretary for Management.

"(I) Overseeing the Component Acquisition Executive organizational structure to ensure Component Acquisition Executives have sufficient capabilities and comply with Department acquisition policies.

"(3) DELEGATION OF CERTAIN ACQUISITION DECISION AUTHORITY.—

"(A) LEVEL 3 ACQUISITIONS.—The Under Secretary for Management may delegate acquisition decision authority to the relevant Component Acquisition Executive for an acquisition program that has a life cycle cost estimate of less than $300,000,000.

"(B) LEVEL 2 ACQUISITIONS.—The Under Secretary for Management may delegate acquisition decision authority in writing to the relevant Component Acquisition Executive for a major acquisition program that has a life cycle cost estimate of at least $300,000 but not more than $1,000,000,000 if all of the following requirements are met:

"(i) The component concerned possesses working policies, processes, and procedures that are consistent with Department-level acquisition policy.

"(ii) The Component Acquisition Executive concerned has adequate, experienced, and dedicated professional employees with program management training, as applicable, commensurate with the size of the acquisition programs and related activities delegated to such Component Ac-

quisition Executive by the Under Secretary for Management.

"(iii) Each major acquisition program concerned has written documentation showing that it has a Department-approved acquisition program baseline and it is meeting agreed-upon cost, schedule, and performance thresholds.

"(C) LEVEL 1 ACQUISITIONS.—The Under Secretary for Management may delegate acquisition decision authority in writing to the relevant Component Acquisition Executive for a Level 1 major acquisition program that has a life cycle cost estimate of more than $1,000,000,000 if all of the following requirements are met:

"(i) The Undersecretary for Management conducts a risk assessment of the planned acquisition and determines that it is appropriate to delegate authority for such major acquisition program.

"(ii) The component concerned possesses working policies, processes, and procedures that are consistent with Department-level acquisition policy.

"(iii) The Component Acquisition Executive concerned has adequate, experienced, and dedicated professional employees with program management training, as applicable, commensurate with the size of the acquisition programs and related activities delegated to such Component Acquisition Executive by the Under Secretary for Management.

"(iv) Each Level 1 major acquisition program concerned has written documentation showing that it has a Department-approved acquisition program baseline and it is meeting agreed-upon cost, schedule, and performance thresholds.

"(v) The Under Secretary for Management provides written notification to the appropriate congressional committees of the decision to delegate the authority to the relevant Component Acquisition Executive.

"(4) RELATIONSHIP TO UNDER SECRETARY FOR SCIENCE AND TECHNOLOGY.—

"(A) IN GENERAL.—Nothing in this subsection shall diminish the authority granted to

the Under Secretary for Science and Technology under this Act. The Under Secretary for Management and the Under Secretary for Science and Technology shall cooperate in matters related to the coordination of acquisitions across the Department so that investments of the Directorate of Science and Technology are able to support current and future requirements of the components of the Department.

''(B) OPERATIONAL TESTING AND EVALUATION.—The Under Secretary for Science and Technology shall—

''(i) ensure, in coordination with relevant component heads, that major acquisition programs—

''(I) complete operational testing and evaluation of technologies and systems to be acquired or developed by major acquisition programs to assess operational effectiveness, suitability, and cybersecurity;

''(II) use independent verification and validation of operational test and evaluation implementation and results, as appropriate; and

"(III) document whether such programs meet all performance requirements included in their acquisition program baselines;

"(ii) ensure that such operational testing and evaluation includes all system components and incorporates operators into the testing to ensure that systems perform as intended in the appropriate operational setting; and

"(iii) determine if testing conducted by other Federal departments and agencies and private entities is relevant and sufficient in determining whether systems perform as intended in the operational setting.".

SEC. 123. ACQUISITION AUTHORITIES FOR UNDER SECRETARY OF STRATEGY, POLICY, AND PLANS.

Subsection (c) of section 709 of the Homeland Security Act of 2002 (6 U.S.C. 349) is amended by—

(1) redesignating paragraphs (4) through (7) as (5) through (8), respectively; and

(2) inserting after paragraph (3) the following new paragraph:

"(4) ensure acquisition programs (as such term is defined in section 836) support the DHS Quadrennial Homeland Security Review Report, the DHS Strategic Plan, the DHS Strategic Priorities, and other appropriate successor documents;".

SEC. 124. ACQUISITION AUTHORITIES FOR PROGRAM ACCOUNTABILITY AND RISK MANAGEMENT (PARM).

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

"SEC. 714. ACQUISITION AUTHORITIES FOR PROGRAM ACCOUNTABILITY AND RISK MANAGEMENT.

"(a) ESTABLISHMENT OF OFFICE.—Within the Management Directorate, there shall be a Program Accountability and Risk Management office to—

"(1) provide consistent accountability, standardization, and transparency of major acquisition programs of the Department;

"(2) serve as the central oversight function for all Department major acquisition programs; and

"(3) provide review and analysis of Department acquisition programs, as appropriate.

1 "(b) RESPONSIBILITIES OF EXECUTIVE DIREC-
2 TOR.—The Program Accountability and Risk Management
3 office shall be led by an Executive Director to oversee the
4 requirements specified in subsection (a). The Executive
5 Director shall report directly to the Under Secretary for
6 Management, and shall carry out the following responsibil-
7 ities:

8 "(1) Monitor regularly the performance of De-
9 partment major acquisition programs between acqui-
10 sition decision events to identify problems with cost,
11 performance, or schedule that components may need
12 to address to prevent cost overruns, performance
13 issues, or schedule delays.

14 "(2) Assist the Under Secretary for Manage-
15 ment in managing the Department's acquisition pro-
16 grams and related activities.

17 "(3) Conduct oversight of individual acquisition
18 programs to implement Department acquisition pro-
19 gram policy, procedures, and guidance with a pri-
20 ority on ensuring the data the office collects and
21 maintains from Department components is accurate
22 and reliable.

23 "(4) Serve as the focal point and coordinator
24 for the acquisition life cycle review process and as

the executive secretariat for the Department's Acquisition Review Board.

''(5) Advise the persons having acquisition decision authority in making acquisition decisions consistent with all applicable laws and in establishing clear lines of authority, accountability, and responsibility for acquisition decisionmaking within the Department.

''(6) Assist the Chief Procurement Officer of the Department, as appropriate, in developing strategies and specific plans for hiring, training, and professional development to address any deficiency within the Department's acquisition workforce.

''(7) Develop standardized certification standards in consultation with the Component Acquisition Executives for all acquisition program managers.

''(8) Assess the results of major acquisition programs' post-implementation reviews and identify opportunities to improve performance throughout the acquisition process.

''(9) Provide technical support and assistance to Department acquisition programs and acquisition personnel and coordinate with the Chief Procurement Officer regarding workforce training and development activities.

"(10) Assist, as appropriate, with the preparation of the Future Years Homeland Security Program, and make such information available to the congressional homeland security committees.

"(c) RESPONSIBILITIES OF COMPONENTS.—Each head of a component shall comply with Federal law, the Federal Acquisition Regulation, and Department acquisition management directives established by the Under Secretary for Management. For each major acquisition program, each head of a component shall—

"(1) define baseline requirements and document changes to such requirements, as appropriate;

"(2) establish a complete life cycle cost estimate with supporting documentation that is consistent with cost estimating best practices as identified by the Comptroller General of the United States;

"(3) verify each life cycle cost estimate against independent cost estimates or assessments, as appropriate, and reconcile any differences;

"(4) complete a cost-benefit analysis with supporting documentation;

"(5) develop and maintain a schedule that is consistent with scheduling best practices as identified by the Comptroller General of the United

States, including, in appropriate cases, an integrated master schedule; and

"(6) ensure that all acquisition program information provided by the component is complete, accurate, timely, and valid.

"(d) DEFINITIONS.—In this section:

"(1) ACQUISITION.—The term 'acquisition' has the meaning given such term in section 131 of title 41, United States Code.

"(2) ACQUISITION DECISION AUTHORITY.—The term 'acquisition decision authority' means the authority, held by the Secretary acting through the Deputy Secretary or Under Secretary for Management to—

"(A) ensure compliance with Federal law, the Federal Acquisition Regulation, and Department acquisition management directives;

"(B) review (including approving, pausing, modifying, or canceling) an acquisition program through the life cycle of such program;

"(C) ensure that acquisition program managers have the resources necessary to successfully execute an approved acquisition program;

"(D) ensure good acquisition program management of cost, schedule, risk, and system

performance of the acquisition program at issue, including assessing acquisition program baseline breaches and directing any corrective action for such breaches; and

''(E) ensure that acquisition program managers, on an ongoing basis, monitor cost, schedule, and performance against established baselines and use tools to assess risks to an acquisition program at all phases of the life cycle of such program to avoid and mitigate acquisition program baseline breaches.

''(3) ACQUISITION DECISION EVENT.—The term 'acquisition decision event', with respect to an acquisition program, means a predetermined point within each of the acquisition phases at which the acquisition decision authority determines whether such acquisition program shall proceed to the next acquisition phase.

''(4) ACQUISITION PROGRAM.—The term 'acquisition program' means the process by which the Department acquires, with any appropriated amounts or fee funding, by contract for purchase or lease, property or services (including construction) that support the missions and goals of the Department.

"(5) ACQUISITION PROGRAM BASELINE.—The term 'acquisition program baseline', with respect to an acquisition program, means a summary of the cost, schedule, and performance parameters, expressed in standard, measurable, quantitative terms, which must be met in order to accomplish the goals of such program.

"(6) BEST PRACTICES.—The term 'best practices', with respect to acquisition, means a knowledge-based approach to capability development that includes the following:

"(A) Identifying and validating needs.

"(B) Assessing alternatives to select the most appropriate solution.

"(C) Clearly establishing well-defined requirements.

"(D) Developing realistic cost assessments and schedules.

"(E) Securing stable funding that matches resources to requirements.

"(F) Demonstrating technology, design, and manufacturing maturity.

"(G) Using milestones and exit criteria or specific accomplishments that demonstrate progress.

"(H) Adopting and executing standardized processes with known success across programs.

"(I) Establishing an adequate workforce that is qualified and sufficient to perform necessary functions.

"(J) Integrating the capabilities described in subparagraphs (A) through (I) into the Department's mission and business operations.

"(7) BREACH.—The term 'breach', with respect to a major acquisition program, means a failure to meet any cost, schedule, or performance threshold specified in the most recently approved acquisition program baseline.

"(8) CONGRESSIONAL HOMELAND SECURITY COMMITTEES.—The term 'congressional homeland security committees' means—

"(A) the Committee on Homeland Security of the House of Representatives and the Committee on Homeland Security and Governmental Affairs of the Senate; and

"(B) the Committee on Appropriations of the House of Representatives and the Committee on Appropriations of the Senate.

"(9) COMPONENT ACQUISITION EXECUTIVE.—The term 'Component Acquisition Executive' means

the senior acquisition official within a component who is designated in writing by the Under Secretary for Management, in consultation with the component head, with authority and responsibility for leading a process and staff to provide acquisition and program management oversight, policy, and guidance to ensure that statutory, regulatory, and higher level policy requirements are fulfilled, including compliance with Federal law, the Federal Acquisition Regulation, and Department acquisition management directives established by the Under Secretary for Management.

''(10) MAJOR ACQUISITION PROGRAM.—The term 'major acquisition program' means a Department acquisition program that is estimated by the Secretary to require an eventual total expenditure of at least $300,000,000 (based on fiscal year 2019 constant dollars) over its life cycle cost or a program identified by the Chief Acquisition Officer as a program of special interest.''.

(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 713, as added by this title, the following new item:

''Sec. 714. Acquisition authorities for Program Accountability and Risk Management.''.

SEC. 125. GOVERNMENT ACCOUNTABILITY OFFICE REVIEW OF BOARD AND OF REQUIREMENTS TO REDUCE DUPLICATION IN ACQUISITION PROGRAMS.

(a) REVIEW REQUIRED.—The Comptroller General of the United States shall conduct a review of the effectiveness of the Acquisition Review Board established under section 836 of the Homeland Security Act of 2002 (as added by this title) and the requirements to reduce unnecessary duplication in acquisition programs established under section 837 of such Act (as added by this title) in improving the Department's acquisition management process.

(b) SCOPE OF REPORT.—The review shall include the following:

(1) An assessment of the effectiveness of the Board in increasing program management oversight, best practices and standards, and discipline among the components of the Department, including in working together and in preventing overlap and unnecessary duplication.

(2) An assessment of the effectiveness of the Board in instilling program management discipline.

(3) A statement of how regularly each major acquisition program is reviewed by the Board, how often the Board stops major acquisition programs

from moving forward in the phases of the acquisition life cycle process, and the number of major acquisition programs that have been halted because of problems with operational effectiveness, schedule delays, or cost overruns.

(4) An assessment of the effectiveness of the Board in impacting acquisition decisionmaking within the Department, including the degree to which the Board impacts decision making within other headquarters mechanisms and bodies involved in the administration of acquisition activities.

(c) REPORT REQUIRED.—Not later than one year after the date of the enactment of this Act, the Comptroller General shall submit to the congressional homeland security committees a report on the review required by this section. The report shall be submitted in unclassified form but may include a classified annex.

SEC. 126. EXCLUDED PARTY LIST SYSTEM WAIVERS.

Not later than five days after the issuance of a waiver by the Secretary of Homeland Security of Federal requirements that an agency not engage in business with a contractor in the Excluded Party List System (or successor system) as maintained by the General Services Administration, the Secretary shall submit to Congress notice of such waiver and an explanation for a finding by the Sec-

retary that a compelling reason exists for issuing such waiver.

SEC. 127. INSPECTOR GENERAL OVERSIGHT OF SUSPENSION AND DEBARMENT.

The Inspector General of the Department of Homeland Security shall—

(1) conduct audits as determined necessary by the Inspector General regarding grant and procurement awards to identify instances in which a contract or grant was improperly awarded to a suspended or debarred entity and whether corrective actions were taken to prevent recurrence; and

(2) review the suspension and debarment program throughout the Department to assess whether suspension and debarment criteria are consistently applied throughout the Department and whether disparities exist in the application of such criteria, particularly with respect to business size and categories.

SEC. 128. CONGRESSIONAL NOTIFICATION FOR MAJOR ACQUISITION PROGRAMS.

(a) IN GENERAL.—Subtitle D of title VIII of the Homeland Security Act of 2002 (6 U.S.C. 391 et seq.), as amended by this title, is further amended by adding at the end the following new section:

"SEC. 837. CONGRESSIONAL NOTIFICATION AND OTHER REQUIREMENTS FOR MAJOR ACQUISITION PROGRAM BREACH.

"(a) REQUIREMENTS WITHIN DEPARTMENT IN EVENT OF BREACH.—

"(1) NOTIFICATIONS.—

"(A) NOTIFICATION OF BREACH.—If a breach occurs in a major acquisition program, the program manager for such program shall notify the Component Acquisition Executive for such program, the head of the component concerned, the Executive Director of the Program Accountability and Risk Management division, the Under Secretary for Management, and the Deputy Secretary not later than 30 calendar days after such breach is identified.

"(B) NOTIFICATION TO SECRETARY.—If a breach occurs in a major acquisition program and such breach results in a cost overrun greater than 15 percent, a schedule delay greater than 180 days, or a failure to meet any of the performance thresholds from the cost, schedule, or performance parameters specified in the most recently approved acquisition program baseline for such program, the Component Acquisition Executive for such program shall no-

tify the Secretary and the Inspector General of the Department not later than five business days after the Component Acquisition Executive for such program, the head of the component concerned, the Executive Director of the Program Accountability and Risk Management Division, the Under Secretary for Management, and the Deputy Secretary are notified of the breach pursuant to subparagraph (A).

"(2) REMEDIATION PLAN AND ROOT CAUSE ANALYSIS.—

"(A) IN GENERAL.—If a breach occurs in a major acquisition program, the program manager for such program shall submit to the head of the component concerned, the Executive Director of the Program Accountability and Risk Management division, and the Under Secretary for Management in writing a remediation plan and root cause analysis relating to such breach and program. Such plan and analysis shall be submitted at a date established at the discretion of the Under Secretary for Management.

"(B) REMEDIATION PLAN.—The remediation plan required under this subparagraph (A) shall—

"(i) explain the circumstances of the breach at issue;

"(ii) provide prior cost estimating information;

"(iii) include a root cause analysis that determines the underlying cause or causes of shortcomings in cost, schedule, or performance of the major acquisition program with respect to which such breach has occurred, including the role, if any, of—

"(I) unrealistic performance expectations;

"(II) unrealistic baseline estimates for cost or schedule or changes in program requirements;

"(III) immature technologies or excessive manufacturing or integration risk;

"(IV) unanticipated design, engineering, manufacturing, or technology integration issues arising during program performance;

"(V) changes to the scope of such program;

"(VI) inadequate program funding or changes in planned out-year funding from one 5-year funding plan to the next 5-year funding plan as outlined in the Future Years Homeland Security Program required under section 874;

"(VII) legislative, legal, or regulatory changes; or

"(VIII) inadequate program management personnel, including lack of sufficient number of staff, training, credentials, certifications, or use of best practices;

"(iv) propose corrective action to address cost growth, schedule delays, or performance issues;

"(v) explain the rationale for why a proposed corrective action is recommended; and

"(vi) in coordination with the Component Acquisition Executive for such program, discuss all options considered, including the estimated impact on cost, schedule, or performance of such program

if no changes are made to current requirements, the estimated cost of such program if requirements are modified, and the extent to which funding from other programs will need to be reduced to cover the cost growth of such program.

"(3) REVIEW OF CORRECTIVE ACTIONS.—

"(A) IN GENERAL.—The Under Secretary for Management shall review the remediation plan required under paragraph (2). The Under Secretary may approve such plan or provide an alternative proposed corrective action within 30 days of the submission of such plan under such paragraph.

"(B) SUBMISSION TO CONGRESS.—Not later than 30 days after the review required under subparagraph (A) is completed, the Under Secretary for Management shall submit to the congressional homeland security committees the following:

"(i) A copy of the remediation plan and the root cause analysis required under paragraph (2).

"(ii) A statement describing the corrective action or actions that have occurred

pursuant to paragraph (2)(b)(iv) for the major acquisition program at issue, with a justification for such action or actions.

"(b) REQUIREMENTS RELATING TO CONGRESSIONAL NOTIFICATION IF BREACH OCCURS.—

"(1) NOTIFICATION TO CONGRESS.—If a notification to the Secretary is made under subsection (a)(1)(B) relating to a breach in a major acquisition program, the Under Secretary for Management shall notify the congressional homeland security committees of such breach in the next quarterly Comprehensive Acquisition Status Report, as required by title I of division D of the Consolidated Appropriations Act, 2016, (Public Law 114–113) following receipt by the Under Secretary of notification under such subsection.

"(2) SIGNIFICANT VARIANCES IN COSTS OR SCHEDULE.—If a likely cost overrun is greater than 20 percent or a likely delay is greater than 12 months from the costs and schedule specified in the acquisition program baseline for a major acquisition program, the Under Secretary for Management shall include in the notification required in paragraph (1) a written certification, with supporting explanation, that—

1 ''(A) such program is essential to the ac-
2 complishment of the Department's mission;
3 ''(B) there are no alternatives to the capa-
4 bility or asset provided by such program that
5 will provide equal or greater capability in both
6 a more cost-effective and timely manner;
7 ''(C) the new acquisition schedule and esti-
8 mates for total acquisition cost are reasonable;
9 and
10 ''(D) the management structure for such
11 program is adequate to manage and control
12 cost, schedule, and performance.
13 ''(c) CONGRESSIONAL HOMELAND SECURITY COM-
14 MITTEES DEFINED.—In this section, the term 'congres-
15 sional homeland security committees' means—
16 ''(1) the Committee on Homeland Security of
17 the House of Representatives and the Committee on
18 Homeland Security and Governmental Affairs of the
19 Senate; and
20 ''(2) the Committee on Appropriations of the
21 House of Representatives and the Committee on Ap-
22 propriations of the Senate.''.
23 (b) CLERICAL AMENDMENT.—The table of contents
24 in section 1(b) of the Homeland Security Act of 2002 is

1 amended by inserting after the item relating to section
2 836, as added by this title, the following new item:

"Sec. 837. Congressional notification and other requirements for major acquisition program breach.".

3 **SEC. 129. MULTIYEAR ACQUISITION STRATEGY.**

4 (a) IN GENERAL.—Subtitle D of title VIII of the
5 Homeland Security Act of 2002 (6 U.S.C. 391 et seq.),
6 as amended by this title, is further amended by adding
7 at the end the following new section:

8 **"SEC. 838. MULTIYEAR ACQUISITION STRATEGY.**

9 "(a) MULTIYEAR ACQUISITION STRATEGY RE-
10 QUIRED.—

11 "(1) IN GENERAL.—Not later than one year
12 after the date of the enactment of this section, the
13 Secretary shall submit to the appropriate congres-
14 sional committees and the Comptroller General of
15 the United States a multiyear acquisition strategy to
16 guide the overall direction of the acquisitions of the
17 Department while allowing flexibility to deal with
18 ever-changing threats and risks, to keep pace with
19 changes in technology that could impact deliverables,
20 and to help industry better understand, plan, and
21 align resources to meet the future acquisition needs
22 of the Department. Such strategy shall be updated
23 and included in each Future Years Homeland Secu-
24 rity Program.

"(2) FORM.—The strategy required under paragraph (1) shall be submitted in unclassified form but may include a classified annex for any sensitive or classified information if necessary. The Secretary shall publish such strategy in an unclassified format that is publicly available.

"(b) CONSULTATION.—In developing the strategy required under subsection (a), the Secretary shall, as the Secretary determines appropriate, consult with headquarters, components, employees in the field, and individuals from industry and the academic community.

"(c) CONTENTS OF STRATEGY.—The strategy shall include the following:

"(1) PRIORITIZED LIST.—A systematic and integrated prioritized list developed by the Under Secretary for Management in coordination with all of the Component Acquisition Executives of Department major acquisition programs that Department and component acquisition investments seek to address, including the expected security and economic benefit of the program or system that is the subject of acquisition and an analysis of how the security and economic benefit derived from such program or system will be measured.

1 "(2) INVENTORY.—A plan to develop a reliable
2 Department-wide inventory of investments and real
3 property assets to help the Department—
4 "(A) plan, budget, schedule, and acquire
5 upgrades of its systems and equipment; and
6 "(B) plan for the acquisition and manage-
7 ment of future systems and equipment.
8 "(3) FUNDING GAPS.—A plan to address fund-
9 ing gaps between funding requirements for major ac-
10 quisition programs and known available resources,
11 including, to the maximum extent practicable, ways
12 of leveraging best practices to identify and eliminate
13 overpayment for items to—
14 "(A) prevent wasteful purchasing;
15 "(B) achieve the greatest level of efficiency
16 and cost savings by rationalizing purchases;
17 "(C) align pricing for similar items; and
18 "(D) utilize purchase timing and econo-
19 mies of scale.
20 "(4) IDENTIFICATION OF CAPABILITIES.—An
21 identification of test, evaluation, modeling, and sim-
22 ulation capabilities that will be required to—
23 "(A) support the acquisition of tech-
24 nologies to meet the needs of such strategy;

"(B) leverage to the greatest extent possible emerging technological trends and research and development trends within the public and private sectors; and

"(C) identify ways to ensure that appropriate technology is acquired and integrated into the Department's operating doctrine to improve mission performance.

"(5) FOCUS ON FLEXIBLE SOLUTIONS.—An assessment of ways the Department can improve its ability to test and acquire innovative solutions to allow needed incentives and protections for appropriate risk-taking in order to meet its acquisition needs with resiliency, agility, and responsiveness to assure homeland security and facilitate trade.

"(6) FOCUS ON INCENTIVES TO SAVE TAXPAYER DOLLARS.—An assessment of ways the Department can develop incentives for program managers and senior Department acquisition officials to—

"(A) prevent cost overruns;

"(B) avoid schedule delays; and

"(C) achieve cost savings in major acquisition programs.

1 "(7) FOCUS ON ADDRESSING DELAYS AND BID
2 PROTESTS.—An assessment of ways the Department
3 can improve the acquisition process to minimize cost
4 overruns in—
5 "(A) requirements development;
6 "(B) procurement announcements;
7 "(C) requests for proposals;
8 "(D) evaluation of proposals;
9 "(E) protests of decisions and awards; and
10 "(F) the use of best practices.
11 "(8) FOCUS ON IMPROVING OUTREACH.—An
12 identification and assessment of ways to increase op-
13 portunities for communication and collaboration with
14 industry, small and disadvantaged businesses, intra-
15 government entities, university centers of excellence,
16 accredited certification and standards development
17 organizations, and national laboratories to ensure
18 that the Department understands the market for
19 technologies, products, and innovation that is avail-
20 able to meet its mission needs and to inform the De-
21 partment's requirements-setting process before en-
22 gaging in an acquisition, including—
23 "(A) methods designed especially to engage
24 small and disadvantaged businesses, a cost-ben-
25 efit analysis of the tradeoffs that small and dis-

1 advantaged businesses provide, information re-
2 lating to barriers to entry for small and dis-
3 advantaged businesses, and information relating
4 to unique requirements for small and disadvan-
5 taged businesses; and
6 ''(B) within the Department Vendor Com-
7 munication Plan and Market Research Guide,
8 instructions for interaction by acquisition pro-
9 gram managers with such entities to—
10 ''(i) prevent misinterpretation of ac-
11 quisition regulations; and
12 ''(ii) permit, within legal and ethical
13 boundaries, interacting with such entities
14 with transparency.
15 ''(9) COMPETITION.—A plan regarding competi-
16 tion under subsection (d).
17 ''(10) ACQUISITION WORKFORCE.—A plan re-
18 garding the Department acquisition workforce under
19 subsection (e).
20 ''(d) COMPETITION PLAN.—The strategy required
21 under subsection (a) shall also include a plan to address
22 actions to ensure competition, or the option of competi-
23 tion, for major acquisition programs. Such plan may in-
24 clude assessments of the following measures in appro-
25 priate cases if such measures are cost effective:

1 ''(1) Competitive prototyping.
2 ''(2) Dual-sourcing.
3 ''(3) Unbundling of contracts.
4 ''(4) Funding of next-generation prototype sys-
5 tems or subsystems.
6 ''(5) Use of modular, open architectures to en-
7 able competition for upgrades.
8 ''(6) Acquisition of complete technical data
9 packages.
10 ''(7) Periodic competitions for subsystem up-
11 grades.
12 ''(8) Licensing of additional suppliers, including
13 small businesses.
14 ''(9) Periodic system or program reviews to ad-
15 dress long-term competitive effects of program deci-
16 sions.
17 ''(e) ACQUISITION WORKFORCE PLAN.—
18 ''(1) ACQUISITION WORKFORCE.—The strategy
19 required under subsection (a) shall also include a
20 plan to address Department acquisition workforce
21 accountability and talent management that identifies
22 the acquisition workforce needs of each component
23 performing acquisition functions and develops op-
24 tions for filling such needs with qualified individuals,

including a cost-benefit analysis of contracting for acquisition assistance.

"(2) ADDITIONAL MATTERS COVERED.—The acquisition workforce plan under this subsection shall address ways to—

"(A) improve the recruitment, hiring, training, and retention of Department acquisition workforce personnel, including contracting officer's representatives, in order to retain highly qualified individuals who have experience in the acquisition life cycle, complex procurements, and management of large programs;

"(B) empower program managers to have the authority to manage their programs in an accountable and transparent manner as such managers work with the acquisition workforce;

"(C) prevent duplication within Department acquisition workforce training and certification requirements through leveraging already-existing training within the Federal Government, academic community, or private industry;

"(D) achieve integration and consistency with Government-wide training and accreditation standards, acquisition training tools, and training facilities;

1 ''(E) designate the acquisition positions
2 that will be necessary to support the Depart-
3 ment acquisition requirements, including in the
4 fields of—
5 ''(i) program management;
6 ''(ii) systems engineering;
7 ''(iii) procurement, including con-
8 tracting;
9 ''(iv) test and evaluation;
10 ''(v) life cycle logistics;
11 ''(vi) cost estimating and program fi-
12 nancial management; and
13 ''(vii) additional disciplines appro-
14 priate to Department mission needs;
15 ''(F) strengthen the performance of con-
16 tracting officers' representatives (as defined in
17 subpart 1.602-2 and subpart 2.101 of the Fed-
18 eral Acquisition Regulation), including by—
19 ''(i) assessing the extent to which
20 such representatives are certified and re-
21 ceive training that is appropriate;
22 ''(ii) assessing what training is most
23 effective with respect to the type and com-
24 plexity of assignment; and

"(iii) implementing actions to improve training based on such assessments; and

"(G) identify ways to increase training for relevant investigators and auditors of the Department to examine fraud in major acquisition programs, including identifying opportunities to leverage existing Government and private sector resources in coordination with the Inspector General of the Department.".

(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 837, as added by this title, the following new item:

"Sec. 838. Multiyear acquisition strategy.".

(c) GOVERNMENT ACCOUNTABILITY OFFICE REVIEW OF MULTI-YEAR ACQUISITION STRATEGY.—

(1) REVIEW.—After submission of the first multiyear acquisition strategy in accordance with section 838 of the Homeland Security Act of 2002, as added by subsection (a), after the date of the enactment of this Act, the Comptroller General of the United States shall conduct a review of such plan within 180 days to analyze the viability of such plan's effectiveness in the following:

(A) Complying with the requirements of such section 838.

(B) Establishing clear connections between Department of Homeland Security objectives and acquisition priorities.

(C) Demonstrating that Department acquisition policy reflects program management best practices and standards.

(D) Ensuring competition or the option of competition for major acquisition programs.

(E) Considering potential cost savings through using already-existing technologies when developing acquisition program requirements.

(F) Preventing duplication within Department acquisition workforce training requirements through leveraging already-existing training within the Federal Government, academic community, or private industry.

(G) Providing incentives for acquisition program managers to reduce acquisition and procurement costs through the use of best practices and disciplined program management.

(2) DEFINITIONS.—The terms ''acquisition'', ''best practices'', and ''major acquisition programs'' have the meanings given such terms in section 836

of the Homeland Security Act of 2002, as added by this title.

(3) REPORT.—Not later than 180 days after the completion of the review required by subsection (a), the Comptroller General of the United States shall submit to the Committee on Homeland Security and the Committee on Appropriations of the House of Representatives and the Committee on Homeland Security and Governmental Affairs and the Committee on Appropriations of the Senate a report on the review. Such report shall be submitted in unclassified form but may include a classified annex.

SEC. 130. ACQUISITION REPORTS.

(a) IN GENERAL.—Subtitle D of title VIII of the Homeland Security Act of 2002 (6 U.S.C. 391 et seq.), as amended by this title, is further amended by adding at the end the following new section:

"SEC. 839. ACQUISITION REPORTS.

"(a) COMPREHENSIVE ACQUISITION STATUS REPORT.—

"(1) IN GENERAL.—At the same time as the President's budget is submitted for a fiscal year under section 1105(a) of title 31, United States Code, the Under Secretary for Management shall

submit to the congressional homeland security committees an annual comprehensive acquisition status report. The report shall include the following:

"(A) The information required under the heading 'Office of the Under Secretary for Management' under title I of division D of the Consolidated Appropriations Act, 2012 (Public Law 112–74) (as required under the Department of Homeland Security Appropriations Act, 2013 (Public Law 113–6)).

"(B) A listing of programs that have been cancelled, modified, paused, or referred to the Under Secretary for Management or Deputy Secretary for additional oversight or action by the Board, Department Office of Inspector General, or the Comptroller General.

"(C) A listing of established Executive Steering Committees, which provide governance of a program or related set of programs and lower-tiered oversight, and support between acquisition decision events and component reviews, including the mission and membership for each.

1 "(2) INFORMATION FOR MAJOR ACQUISITION
2 PROGRAMS.—For each major acquisition program,
3 the report shall include the following:
4 "(A) A narrative description, including
5 current gaps and shortfalls, the capabilities to
6 be fielded, and the number of planned incre-
7 ments or units.
8 "(B) Acquisition Review Board (or other
9 board designated to review the acquisition) sta-
10 tus of each acquisition, including the current
11 acquisition phase, the date of the last review,
12 and a listing of the required documents that
13 have been reviewed with the dates reviewed or
14 approved.
15 "(C) The most current, approved acquisi-
16 tion program baseline (including project sched-
17 ules and events).
18 "(D) A comparison of the original acquisi-
19 tion program baseline, the current acquisition
20 program baseline, and the current estimate.
21 "(E) Whether or not an independent
22 verification and validation has been imple-
23 mented, with an explanation for the decision
24 and a summary of any findings.

"(F) A rating of cost risk, schedule risk, and technical risk associated with the program (including narrative descriptions and mitigation actions).

"(G) Contract status (including earned value management data as applicable).

"(H) A lifecycle cost of the acquisition, and time basis for the estimate.

"(3) UPDATES.—The Under Secretary shall submit quarterly updates to such report not later than 45 days after the completion of each quarter.

"(b) QUARTERLY PROGRAM ACCOUNTABILITY REPORT.—The Under Secretary for Management shall prepare a quarterly program accountability report to meet the mandate of the Department to perform program health assessments and improve program execution and governance. The report shall be submitted to the congressional homeland security committees.

"(c) CONGRESSIONAL HOMELAND SECURITY COMMITTEES DEFINED.—In this section, the term 'congressional homeland security committees' means—

"(1) the Committee on Homeland Security of the House of Representatives and the Committee on Homeland Security and Governmental Affairs of the Senate; and

"(2) the Committee on Appropriations of the House of Representatives and the Committee on Appropriations of the Senate.".

(b) LEVEL 3 ACQUISITION PROGRAMS OF COMPONENTS OF THE DEPARTMENT.—

(1) IN GENERAL.—Not later than 60 days after the date of the enactment of this Act, component heads of the Department of Homeland Security shall identify to the Under Secretary for Management of the Department all level 3 acquisition programs of each respective component. Not later than 30 days after receipt of such information, the Under Secretary shall certify in writing to the congressional homeland security committees whether such component heads have properly identified such programs. To carry out this paragraph, the Under Secretary shall establish a process with a repeatable methodology to continually identify level 3 acquisition programs.

(2) POLICIES AND GUIDANCE.—Not later than 180 days after the date of the enactment of this Act, component heads of the Department of Homeland Security shall submit to the Under Secretary for Management of the Department their respective policies and relevant guidance for level 3 acquisition

programs of each respective component. Not later than 90 days after receipt of such policies and guidance, the Under Secretary for Management shall certify to the congressional homeland security committees that each component's respective policies and guidance adhere to Department-wide acquisition policies.

(c) CLERICAL AMENDMENT.—The table of contents in section 1(b) of such Act is amended by inserting after the item relating to section 838, as added by this title, the following new item:

"Sec. 839. Acquisition reports.".

SEC. 131. PROHIBITION ON OPERATION OR PROCUREMENT OF FOREIGN-MADE UNMANNED AIRCRAFT SYSTEMS.

(a) PROHIBITION ON AGENCY OPERATION OR PROCUREMENT.—The Secretary of Homeland Security may not operate, provide financial assistance for, or enter into or renew a contract for the procurement of—

(1) an unmanned aircraft system (UAS) that—

(A) is manufactured in a covered foreign country or by a corporation domiciled in a covered foreign country;

(B) uses flight controllers, radios, data transmission devices, cameras, or gimbals manufactured in a covered foreign country or by a

corporation domiciled in a covered foreign country;

(C) uses a ground control system or operating software developed in a covered foreign country or by a corporation domiciled in a covered foreign country; or

(D) uses network connectivity or data storage located in or administered by a corporation domiciled in a covered foreign country; or

(2) a system manufactured in a covered foreign country or by a corporation domiciled in a covered foreign country for the detection or identification of covered unmanned aircraft systems.

(b) WAIVER.—The Secretary of Homeland Security may waive the prohibition under subsection (a) on a case by case basis by certifying in writing to the Committee on Homeland Security of the House of Representatives and the Committee on Homeland Security and Governmental Affairs of the Senate that the operation or procurement that is the subject of such a waiver is required—

(1) in the national interest of the United States;

(2) for counter-UAS surrogate testing and training; or

(3) for intelligence, electronic warfare, or information warfare operations, testing, analysis, and or training.

(c) DEFINITIONS.—In this section:

(1) COVERED FOREIGN COUNTRY.—The term ''covered foreign country'' means a country labeled as a strategic competitor in the ''Summary of the 2018 National Defense Strategy of the United States of America: Sharpening the American Military's Competitive Edge'' issued by the Department of Defense pursuant to section 113 of title 10, United States Code.

(2) COVERED UNMANNED AIRCRAFT SYSTEM.—The term ''unmanned aircraft system'' has the meaning given such term in section 331 of the FAA Modernization and Reform Act of 2012 (Public Law 112–95; 49 U.S.C. 44802 note).

SEC. 132. ESTABLISHMENT OF THE OFFICE OF BIOMETRIC IDENTITY MANAGEMENT.

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

"SEC. 715. OFFICE OF BIOMETRIC IDENTITY MANAGEMENT.

"(a) ESTABLISHMENT.—The Office of Biometric Identity Management is established within the Management Directorate of the Department.

"(b) DIRECTOR.—

"(1) IN GENERAL.—The Office of Biometric Identity Management shall be administered by the Director of the Office of Biometric Identity Management (in this section referred to as the 'Director') who shall report to the Secretary, or to another official of the Department, as the Secretary may direct.

"(2) QUALIFICATIONS AND DUTIES.—The Director shall—

"(A) have significant professional management experience, as well as experience in the field of biometrics and identity management;

"(B) lead the Department's biometric identity services to support efforts and activities relating to anti-terrorism, counter-terrorism, border security, credentialing, national security, and public safety;

"(C) enable operational missions across the Department by receiving, matching, storing, sharing, and analyzing biometric and associated biographic and encounter data;

1 ''(D) deliver biometric identity information
2 and analysis capabilities to—
3 ''(i) the Department and its compo-
4 nents;
5 ''(ii) appropriate Federal, State, local,
6 and tribal agencies;
7 ''(iii) appropriate foreign govern-
8 ments; and
9 ''(iv) appropriate private sector enti-
10 ties;
11 ''(E) support the law enforcement, public
12 safety, national security, and homeland security
13 missions of other Federal, State, local, and trib-
14 al agencies, as appropriate;
15 ''(F) manage the operation of the Depart-
16 ment's primary biometric repository and identi-
17 fication system;
18 ''(G) manage Biometric Support Centers
19 to provide biometric identification and
20 verification analysis and services to the Depart-
21 ment, appropriate Federal, State, local, and
22 tribal agencies, appropriate foreign govern-
23 ments, and appropriate private sector entities;
24 ''(H) oversee the implementation of De-
25 partment-wide standards for biometric con-

formity, and work to make such standards Government-wide;

"(I) in coordination with the Department's Office of Strategy, Policy, and Plans, and in consultation with relevant component offices and headquarters offices, enter into data sharing agreements with appropriate Federal, State, local, and foreign agencies to support immigration, law enforcement, national security, and public safety missions;

"(J) maximize interoperability with other Federal, State, local, and foreign biometric systems, as appropriate;

"(K) ensure the activities of the Office of Biometric Identity Management are carried out in compliance with the policies and procedures established by the Privacy Officer appointed under section 222; and

"(L) carry out other duties and powers prescribed by law or delegated by the Secretary.

"(c) DEPUTY DIRECTOR.—There shall be in the Office of Biometric Identity Management a Deputy Director, who shall assist the Director in the management of the Office.

"(d) OTHER AUTHORITIES.—

"(1) IN GENERAL.—The Director may establish such other offices within the Office of Biometric Identity Management as the Director determines necessary to carry out the missions, duties, functions, and authorities of the Office.

"(2) NOTIFICATION.—If the Director exercises the authority provided by paragraph (1), the Director shall notify the Committee on Homeland Security of the House of Representatives and the Committee on Homeland Security and Governmental Affairs of the Senate not later than 30 days before exercising such authority.".

(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 714, as added by this title, the following new item:

"Sec. 715. Office of Biometric Identity Management.".

Subtitle C—Management of Programs

SEC. 141. DEPARTMENT OF HOMELAND SECURITY ENHANCED HIRING.

(a) APPOINTMENT AUTHORITY FOR VETERANS.—Notwithstanding sections 3309 through 3319, 3327, and 3330 of title 5, United States Code, the Secretary of Homeland Security may noncompetitively appoint a quali-

1 fied veteran to a position in the competitive service within
2 the Department of Homeland Security.
3 (b) PUBLIC HIRING AUTHORITY.—
4 (1) IN GENERAL.—The Secretary of Homeland
5 Security may, notwithstanding sections 3309
6 through 3319, 3327, and 3330 of title 5, United
7 States Code, noncompetitively appoint a qualified
8 candidate to a position in the competitive service if
9 the Secretary determines such position is critical to
10 the mission of the Department.
11 (2) CONDITIONS.—
12 (A) 20 PERCENT OR GREATER.—The Sec-
13 retary of Homeland Security may exercise the
14 authority under paragraph (1) in any calendar
15 year only if the representation of veterans with-
16 in the Department of Homeland Security civil-
17 ian workforce at the end of the preceding fiscal
18 year was 20 percent or greater.
19 (B) LESS THAN 20 PERCENT.—In the
20 event the representation of veterans within the
21 Department of Homeland Security in a fiscal
22 year does not meet or exceed the level identified
23 in subparagraph (A), the Secretary may exer-
24 cise the authority under this section for the fol-
25 lowing calendar year provided that the total

number of qualified candidates appointed under this section does not exceed 20 percent of the total number of positions that the Department of Homeland Security filled during the preceding fiscal year.

(c) REGULATIONS.—The Secretary of Homeland Security may prescribe regulations to carry out this section and any such regulations shall be exempt from the requirements of section 553 of title 5, United States Code, as a matter relating to agency management or personnel.

(d) INFORMATION AND REPORT.—

(1) INFORMATION.—The Secretary of Homeland Security shall, not later than December 31 of each calendar year, provide to the Director of the Office of Personnel Management identification of the mission critical occupations to which the Secretary appointed qualified candidates under subsection (b) during the preceding fiscal year.

(2) REPORT.—The Secretary of Homeland Security shall annually report to Congress on the effectiveness of the use of the authority under this section regarding the length of time to hire individuals, employee retention, and vacancies within the Department of Homeland Security.

(e) DEFINITIONS.—In this section—

(1) the term ''veteran'' means an individual who—

(A)(i) has served on active duty in the Armed Forces; and

(ii) was discharged or released from active duty in the Armed Forces under honorable conditions; or

(B) is preference eligible, as defined in section 2108 of title 5, United States Code; and

(2) the term ''mission critical occupation'' means those occupations that affect the ability to achieve the agency's mission.

SEC. 142. FITNESS STANDARDS.

(a) STRATEGY FOR FITNESS STANDARDIZATION.—Not later than 180 days after the date of the enactment of this Act, the Secretary of Homeland Security, acting through the Chief Security Officer of the Department of Homeland Security and in coordination with heads of the components of the Department, shall—

(1) develop a strategy and timeline for implementation and use of uniform fitness standards that correspond to the relevant position risk level as the basis for fitness determinations for a contractor employee across the Department of Homeland Security; and

(2) ensure such strategy includes a system of reciprocity across the Department.

(b) LENGTH OF TIME FOR FITNESS REVIEW.—The Secretary of Homeland Security, acting through the Chief Security Officer of the Department of Homeland Security, shall collect data to allow the Department and its components and contractor representatives to assess average fitness investigation, adjudication, and determination processing times for each component of the Department, including information regarding the parameters used to calculate each such average.

(c) STUDY ON FITNESS ADJUDICATION STATUS UPDATES.—Not later than one year after the date of the enactment of this Act, the Secretary of Homeland Security, acting through the Chief Security Officer of the Department of Homeland Security, shall enter into a contract with a federally funded research and development center (FFRDC) to conduct a cost benefit analysis for establishing a uniform process to provide contractor representatives access to information regarding the status of fitness determinations for Department contractor employees relevant to such contractor representatives.

SEC. 143. TRAINING TO PROTECT THE VULNERABLE.

(a) TRAINING EXPANSION.—Section 884(c) of the Homeland Security Act of 2002 (6 U.S.C. 464) is amended—

(1) in paragraph (9), by striking ''and'' at the end;

(2) by redesignating paragraph (10) as paragraph (11); and

(3) by inserting after paragraph (9) and inserting the following new paragraphs:

''(10) conduct training programs for Federal, State, local, Tribal, and territorial law enforcement agencies related to human smuggling and trafficking along the United States border, at airport security checkpoints, and within the interior of the United States; and''.

(b) FLETC HUMAN TRAFFICKING AWARENESS TRAINING PROGRAM.—The Director, in consultation with the Blue Campaign office, shall develop a program to provide training to Federal, State, local, Tribal, territorial, and international law enforcement personnel, as appropriate, related to—

(1) identifying instances of human trafficking;

(2) the types of information that should be collected and recorded in information technology systems utilized by the Department to help identify in-

1 dividuals suspected or convicted of human traf-
2 ficking;
3 (3) how to conduct systematic and routine in-
4 formation sharing within the Department and
5 among Federal, State, Tribal, and local law enforce-
6 ment agencies regarding—
7 (A) individuals suspected or convicted of
8 human trafficking; and
9 (B) patterns and practices of human traf-
10 ficking;
11 (4) techniques to identify suspected victims of
12 trafficking along the United States border and at
13 airport security checkpoints;
14 (5) methods to be used by the Transportation
15 Security Administration and personnel from other
16 appropriate agencies to—
17 (A) train employees of the Transportation
18 Security Administration to identify suspected
19 victims of trafficking; and
20 (B) serve as a liaison and resource regard-
21 ing human trafficking prevention to appropriate
22 State, local, and private sector aviation workers
23 and the traveling public.

SEC. 144. DEPARTMENT OF HOMELAND SECURITY BLUE CAMPAIGN ENHANCEMENT.

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

1 "(D) The Federal Law Enforcement
2 Training Center.
3 "(E) The United States Secret Service.
4 "(F) Any other components or offices the
5 Secretary determines appropriate.
6 "(2) CONSULTATION.—The Director shall con-
7 sult the Board established pursuant to paragraph
8 (1) regarding the following:
9 "(A) Trends and patterns in human traf-
10 ficking to inform the development of training
11 and materials by the Blue Campaign.
12 "(B) The development of effective aware-
13 ness campaigns for Federal and non-Federal of-
14 ficials to identify and prevent instances of
15 human trafficking.
16 "(C) Outreach to persons or entities that
17 may be uniquely positioned to recognize signs of
18 human trafficking and provide assistance in the
19 development of materials for such persons.
20 "(3) APPLICABILITY.—The Federal Advisor
21 Committee Act (5 U.S.C. App.) does not apply to—
22 "(A) the Board; or
23 "(B) consultations under paragraph (2).
24 "(h) CONSULTATION.—With regard to the develop-
25 ment of programs under the Blue Campaign and the im-

plementation of such programs, the Director is authorized to consult with State, local, Tribal, and territorial agencies, non-governmental organizations, private sector organizations, and experts. Such consultation shall be exempt from the Federal Advisory Committee Act (5 U.S.C. App.).''.

TITLE II—INTELLIGENCE AND INFORMATION SHARING

Subtitle A—DHS Intelligence Enterprise

SEC. 201. ANNUAL HOMELAND THREAT ASSESSMENTS.

(a) IN GENERAL.—Subtitle A of title II of the Homeland Security Act of 2002 (6 U.S.C. 121 et seq.) is amended by adding at the end the following new section:

''SEC. 210H. HOMELAND THREAT ASSESSMENTS.

''(a) IN GENERAL.—Not later than 180 days after the date of the enactment of this section and for each of the next five fiscal years (beginning in the fiscal year that begins after the date of the enactment of this section) the Secretary, acting through the Under Secretary for Intelligence and Analysis, and using departmental information, including component information, and information provided through State and major urban area fusion centers, shall conduct an assessment of the terrorist threat to the homeland.

1 ''(b) CONTENTS.—Each assessment under subsection
2 (a) shall include the following:
3 ''(1) Empirical data assessing terrorist activi-
4 ties and incidents over time in the United States, in-
5 cluding terrorist activities and incidents planned or
6 supported by persons outside of the United States
7 targeting the homeland.
8 ''(2) An evaluation of current terrorist tactics,
9 as well as ongoing and possible future changes in
10 terrorist tactics.
11 ''(3) An assessment of criminal activity encoun-
12 tered or observed by officers or employees of compo-
13 nents in the field which is suspected of financing ter-
14 rorist activity.
15 ''(4) Detailed information on all individuals de-
16 nied entry to or removed from the United States as
17 a result of material support provided to a foreign
18 terrorist organization (as such term is used in sec-
19 tion 219 of the Immigration and Nationality Act (8
20 U.S.C. 1189)).
21 ''(5) The efficacy and spread of foreign ter-
22 rorist organization propaganda, messaging, or re-
23 cruitment.

1 ''(6) An assessment of threats, including cyber
2 threats, to the homeland, including to critical infra-
3 structure and Federal civilian networks.
4 ''(7) An assessment of current and potential
5 terrorism and criminal threats posed by individuals
6 and organized groups seeking to unlawfully enter the
7 United States.
8 ''(8) An assessment of threats to the transpor-
9 tation sector, including surface and aviation trans-
10 portation systems.
11 ''(c) ADDITIONAL INFORMATION.—The assessments
12 required under subsection (a)—
13 ''(1) shall, to the extent practicable, utilize ex-
14 isting component data collected from the field; and
15 ''(2) may incorporate relevant information and
16 analysis from other agencies of the Federal Govern-
17 ment, agencies of State and local governments (in-
18 cluding law enforcement agencies), as well as the
19 private sector, disseminated in accordance with
20 standard information sharing procedures and poli-
21 cies.
22 ''(d) FORM.—The assessments required under sub-
23 section (a) shall be shared with the appropriate congres-
24 sional committees and submitted in classified form, but—
25 ''(1) shall include unclassified summaries; and

"(2) may include unclassified annexes, if appropriate.".

(b) CONFORMING AMENDMENT.—Subsection (d) of section 201 of the Homeland Security Act of 2002 (6 U.S.C. 121) is amended by adding at the end the following new paragraph:

"(24) To carry out section 210H (relating to homeland threat assessments).".

(c) CLERICAL AMENDMENT.—The table of contents of the Homeland Security Act of 2002 is amended by inserting after the item relating to section 210G the following new item:

"Sec. 210H. Homeland threat assessments.".

SEC. 202. HOMELAND INTELLIGENCE DOCTRINE.

(a) IN GENERAL.—Subtitle A of title II of the Homeland Security Act of 2002 (6 U.S.C. 121 et seq.), as amended by this title, is further amended by adding at the end the following new section:

"SEC. 210I. HOMELAND INTELLIGENCE DOCTRINE.

"(a) IN GENERAL.—Not later than 180 days after the date of the enactment of this section, the Secretary, acting through the Chief Intelligence Officer of the Department, in coordination with intelligence components of the Department, the Office of the General Counsel, the Privacy Office, and the Office for Civil Rights and Civil Liberties, shall develop and disseminate written Depart-

1 ment-wide guidance for the processing, analysis, produc-
2 tion, and dissemination of homeland security information
3 (as such term is defined in section 892) and terrorism in-
4 formation (as such term is defined in section 1016 of the
5 Intelligence Reform and Terrorism Prevention Act of
6 2004 (6 U.S.C. 485)).

7 ''(b) CONTENTS.—The guidance required under sub-
8 section (a) shall, at a minimum, include the following:

9 ''(1) A description of guiding principles and
10 purposes of the Department's intelligence enterprise.

11 ''(2) A summary of the roles, responsibilities,
12 and programs of each intelligence component of the
13 Department in the processing, analysis, production,
14 or dissemination of homeland security information
15 and terrorism information, including relevant au-
16 thorities and restrictions applicable to each such in-
17 telligence component.

18 ''(3) Guidance for the processing, analysis, and
19 production of such information.

20 ''(4) Guidance for training necessary for appro-
21 priate personnel to process, analyze, produce, and
22 disseminate homeland security information and ter-
23 rorism information.

24 ''(5) Guidance for the dissemination of such in-
25 formation, including within the Department, among

and between Federal departments and agencies, among and between State, local, Tribal, and territorial governments, including law enforcement, and with foreign partners and the private sector, consistent with the protection of privacy, civil rights, and civil liberties.

''(6) A description of how the dissemination to the intelligence community (as such term is defined in section 3(4) of the National Security Act of 1947 (50 U.S.C. 3003(4))) and Federal law enforcement of such information assists such entities in carrying out their respective missions.

''(c) FORM.—The guidance required under subsection (a) shall be submitted in unclassified form, but may include a classified annex.

''(d) ANNUAL REVIEW.—For each of the 5 fiscal years beginning with the first fiscal year that begins after the date of the enactment of this section, the Secretary shall conduct a review of the guidance required under subsection (a) and, as appropriate, revise such guidance.''.

(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 210H, as added by title, the following new item:

''Sec. 210I. Homeland intelligence doctrine.''.

SEC. 203. COMPTROLLER GENERAL ASSESSMENT.

(a) ANNUAL ASSESSMENT REQUIRED.—Not later than 1 year after the date of the enactment of this Act and again not later than 5 years thereafter, 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 an assessment of the degree to which guidance established pursuant to section 210I of the Homeland Security Act of 2002 (as added by section 202) is implemented across the Department of Homeland Security. Such assessment should evaluate the extent to which such guidance is carried out in a manner that protects privacy, civil rights, and civil liberties.

(b) ELEMENTS OF ASSESSMENT.—In conducting each assessment under subsection (a), the Comptroller General of the United States shall—

(1) use standard methodology and reporting formats in order to demonstrate and display any changes over time; and

(2) include any other subject matter the Comptroller General determines appropriate.

(c) ACCESS TO RELEVANT DATA.—To carry out this section, the Secretary of Homeland Security shall ensure that the Comptroller General of the United States has access to all relevant data.

SEC. 204. ANALYSTS FOR THE CHIEF INTELLIGENCE OFFICER.

Paragraph (1) of section 201(e) of the Homeland Security Act of 2002 (6 U.S.C. 121(e)) is amended by adding at the end the following new sentence: ''The Secretary shall also provide the Chief Intelligence Officer with a staff having appropriate expertise and experience to assist the Chief Intelligence Officer.''.

SEC. 205. ESTABLISHMENT OF INSIDER THREAT PROGRAM.

(a) IN GENERAL.—Title I of the Homeland Security Act of 2002 (6 U.S.C. 111 et seq.) is amended by adding at the end the following new section:

''SEC. 104. INSIDER THREAT PROGRAM.

''(a) ESTABLISHMENT.—The Secretary shall establish an Insider Threat Program within the Department. Such Program shall—

''(1) provide training and education for Department personnel to identify, prevent, mitigate, and respond to insider threat risks to the Department's critical assets;

''(2) provide investigative support regarding potential insider threats that may pose a risk to the Department's critical assets; and

''(3) conduct risk mitigation activities for insider threats.

''(b) STEERING COMMITTEE.—

"(1) IN GENERAL.—The Secretary shall establish a Steering Committee within the Department. The Under Secretary for Intelligence and Analysis shall serve as the Chair of the Steering Committee. The Chief Security Officer shall serve as the Vice Chair. The Steering Committee shall be comprised of representatives of the Office of Intelligence and Analysis, the Office of the Chief Information Officer, the Office of the General Counsel, the Office for Civil Rights and Civil Liberties, the Privacy Office, the Office of the Chief Human Capital Officer, the Office of the Chief Financial Officer, the Federal Protective Service, the Office of the Chief Procurement Officer, the Science and Technology Directorate, and other components or offices of the Department as appropriate. Such representatives shall meet on a regular basis to discuss cases and issues related to insider threats to the Department's critical assets, in accordance with subsection (a).

"(2) RESPONSIBILITIES.—Not later than one year after the date of the enactment of this section, the Under Secretary for Intelligence and Analysis and the Chief Security Officer, in coordination with the Steering Committee established pursuant to paragraph (1), shall carry out the following:

1 ''(A) Develop a holistic strategy for De-
2 partment-wide efforts to identify, prevent, miti-
3 gate, and respond to insider threats to the De-
4 partment's critical assets.
5 ''(B) Develop a plan to implement the in-
6 sider threat measures identified in the strategy
7 developed under subparagraph (A) across the
8 components and offices of the Department.
9 ''(C) Document insider threat policies and
10 controls.
11 ''(D) Conduct a baseline risk assessment of
12 insider threats posed to the Department's crit-
13 ical assets.
14 ''(E) Examine existing programmatic and
15 technology best practices adopted by the Fed-
16 eral Government, industry, and research insti-
17 tutions to implement solutions that are vali-
18 dated and cost-effective.
19 ''(F) Develop a timeline for deploying
20 workplace monitoring technologies, employee
21 awareness campaigns, and education and train-
22 ing programs related to identifying, preventing,
23 mitigating, and responding to potential insider
24 threats to the Department's critical assets.

1 ''(G) Require the Chair and Vice Chair of
2 the Steering Committee to consult with the
3 Under Secretary for Science and Technology
4 and other appropriate stakeholders to ensure
5 the Insider Threat Program is informed, on an
6 ongoing basis, by current information regarding
7 threats, beset practices, and available tech-
8 nology.
9 ''(H) Develop, collect, and report metrics
10 on the effectiveness of the Department's insider
11 threat mitigation efforts.
12 ''(c) DEFINITIONS.—In this section:
13 ''(1) CRITICAL ASSETS.—The term 'critical as-
14 sets' means the people, facilities, information, and
15 technology required for the Department to fulfill its
16 mission.
17 ''(2) INSIDER.—The term 'insider' means—
18 ''(A) any person who has access to classi-
19 fied national security information and is em-
20 ployed by, detailed to, or assigned to the De-
21 partment, including members of the Armed
22 Forces, experts or consultants to the Depart-
23 ment, industrial or commercial contractors, li-
24 censees, certificate holders, or grantees of the
25 Department, including all subcontractors, per-

sonal services contractors, or any other category of person who acts for or on behalf of the Department, as determined by the Secretary; or

"(B) State, local, Tribal, territorial, and private sector personnel who possess security clearances granted by the Department.

"(3) INSIDER THREAT.—The term 'insider threat' means the threat that an insider will use his or her authorized access, wittingly or unwittingly, to do harm to the security of the United States, including damage to the United States through espionage, terrorism, the unauthorized disclosure of classified national security information, or through the loss or degradation of departmental resources or capabilities.".

(b) REPORTING.—

(1) IN GENERAL.—Not later than two years after the date of the enactment of section 104 of the Homeland Security Act of 2002 (as added by subsection (a) of this section) and biennially thereafter for the next four years, the Secretary of Homeland Security shall submit to the Committee on Homeland Security and the Permanent Select Committee on Intelligence of the House of Representatives and the Committee on Homeland Security and Govern-

mental Affairs and the Select Committee on Intelligence of the Senate a report on how the Department of Homeland Security and its components and offices have implemented the strategy developed pursuant to subsection (b)(2)(A) of such section 104, the status of the Department's risk assessment of critical assets, the types of insider threat training conducted, the number of Department employees who have received such training, and information on the effectiveness of the Insider Threat Program (established pursuant to subsection (a) of such section 104), based on metrics developed, collected, and reported pursuant to subsection (b)(2)(H) of such section 104.

(2) DEFINITIONS.—In this subsection, the terms ''critical assets'', ''insider'', and ''insider threat'' have the meanings given such terms in section 104 of the Homeland Security Act of 2002 (as added by subsection (a) of this section).

(c) 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 103 the following new item:

''Sec. 104. Insider Threat Program.''.

SEC. 206. DEPARTMENT OF HOMELAND SECURITY COUNTERINTELLIGENCE VETTING TASK FORCE.

(a) ESTABLISHMENT.—Not later than 180 days after the date of the enactment of this Act, the Secretary of Homeland Security shall assign personnel of the Department of Homeland Security to participate in a counterintelligence vetting task force to make recommendations to improve counterintelligence vetting for appropriate departmental programs.

(b) PERSONNEL.—In carrying out subsection (a), the Secretary of Homeland Security may assign personnel from any component of the Department of Homeland Security the Secretary determines necessary to participate in the task force established pursuant to such subsection.

(c) COORDINATION.—In carrying out subsection (a), the Secretary of Homeland Security may request participation in the task force established pursuant to such subsection from other appropriate Federal agencies.

(d) REPORT.—Not later than one year after the date of the enactment of this Act, the Secretary 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 the recommendations made by the task force established pursuant to subsection (a).

SEC. 207. VISA SECURITY.

(a) ESTABLISHMENT.—

(1) IN GENERAL.—Not later than 90 days after the date of the enactment of this Act, the interagency working group established under section 1746(a) of the National Defense Authorization Act for Fiscal Year 2020 (Public Law 116–92) shall commence a review of the current policies and procedures of the Department of Homeland Security and Department of State for the purpose of identifying, investigating, and preventing the illicit transfer of sensitive technologies and research from United States institutions of higher education and research institutions through more effective visa security operations and improved protections for such sensitive technologies.

(2) OBJECTIVES.—

(A) ANALYSIS OF CURRENT VISA ISSUANCE AND ADMISSION PROCEDURES.—The interagency working group referred to in paragraph (1) shall—

(i) analyze the current visa application process, and the role of the Department of Homeland Security and the Department of State in such process, including the screening of visa applicants against

appropriate criminal, intelligence, national security, terrorism, and other databases and information maintained by the Federal Government, and make recommendations to the Secretaries of such Departments to better screen, identify, and refuse entry to individuals who seek to enter the United States to engage in the illicit transfer of sensitive technologies from United States institutions of higher educations or research institutions;

(ii) evaluate current policies for refusing visas on grounds that an individual is likely to enter the United States to engage in the illicit transfer of sensitive technologies and recommend updates to the Foreign Affairs Manual and other agency guidance to clarify when and how visas can be refused on such grounds; and

(iii) analyze current screening procedures at United States ports of entry and make recommendations to the Secretaries of such Departments to better identify individuals who seek to enter the United

States to engage in such illicit transfer of sensitive technologies.

(B) NATIONAL SECURITY REVIEW OF CERTAIN NONIMMIGRANT STUDENTS.—The interagency working group shall recommend procedures and standards for the Department of Homeland Security, in cooperation with other appropriate Federal agencies, to conduct national security reviews of aliens who—

(i) are present in the United States—

(I) in a nonimmigrant classification described in subparagraphs (F), (J), or (M) of section 101(a)(15) of the Immigration and Nationality Act (8 U.S.C. 1101(a)(15)) and change from a program of study not related to sensitive technologies to a program of study or significant coursework, research, or laboratory access related to sensitive technologies; or

(II) as a nonimmigrant and seek to change status, pursuant to section 248 of the Immigration and Nationality Act (8 U.S.C. 1258)), to that of a nonimmigrant described in subpara-

graph (F), (J), or (M) of section 101(a)(15) of such Act (8 U.S.C. 1101(a)(15)), for purposes of engaging in a program of study related to sensitive technologies; and

(ii) as a result of engaging in a program of study related to sensitive technologies, will have access to information related to operating, installing, maintaining, repairing, overhauling, or refurbishing sensitive technologies or development activities related to sensitive technologies.

(C) IDENTIFYING INDIVIDUALS REQUIRING NATIONAL SECURITY REVIEW.—For purposes of facilitating the identification of individuals described in subparagraph (B)(ii), the interagency working group shall—

(i) develop a nonpublic list of six-digit Classification of Instructional Programs (CIP) codes for programs of study related to sensitive technologies to be used in reporting required by section 641 of the Immigration and Nationality Act (8 U.S.C. 1372(d)) and related regulations;

(ii) recommend to the Secretary of Homeland Security changes, as appropriate, to the Student and Exchange Visitor Information System, or other system designated for such purpose by the Secretary of Homeland Security, to ensure that individuals who seek to engage in programs of study but who will not have access to information related to operating, installing, maintaining, repairing, overhauling, or refurbishing sensitive technologies or development activities related to sensitive technologies are not unnecessarily subjected to national security reviews;

(iii) recommend to the Secretary of Homeland Security changes to relevant regulations to ensure that entities certified by the Student and Exchange Visitor Program routinely and accurately report the program of study and other necessary information in the Student and Exchange Visitor Information System, or other system designated for such purpose by the Secretary of Homeland Security, for each

nonimmigrant described in subparagraph (F), (J), or (M) of section 101(a)(15) of the Immigration and Nationality Act (8 U.S.C. 1101(a)(15)) who is enrolled in such entity; and

(iv) identify mechanisms for the Department of Homeland Security, in cooperation with other appropriate Federal agencies, to order the removal of and make ineligible for future nonimmigrant classification described in subparagraphs (F), (J), or (M) of section 101(a)(15) of the Immigration and Nationality Act (8 U.S.C. 1101(a)(15)) individuals who may be identified following pursuant to national security reviews conducted in accordance with subparagraph (B).

(D) IDENTIFYING GAPS IN AUTHORITY TO ADDRESS NATIONAL SECURITY THREATS.—Not later than one year after the date of the enactment of this Act, the interagency working group shall identify deficiencies in existing legal authorities determined to be an impediment in achieving the recommendations described in clauses (ii) and (iii) of subparagraph (C), and

1 recommend to the appropriate congressional
2 committees legislative solutions to address such
3 deficiencies.
4 (3) COMPOSITION.—In addition to the members
5 specified in section 1746(a)(2) of the National De-
6 fense Authorization Act for Fiscal Year 2020 (Pub-
7 lic Law 116–92), for purposes of carrying out the
8 review required under paragraph (1), the inter-
9 agency working group consult with the following:
10 (A) U.S. Customs and Border Protection,
11 Office of Field Operations.
12 (B) U.S. Immigration and Customs En-
13 forcement, Student and Exchange Visitor Pro-
14 gram.
15 (C) U.S. Immigration and Customs En-
16 forcement, Counterterrorism and Criminal Ex-
17 ploitation Unit.
18 (D) U.S. Immigration and Customs En-
19 forcement, Visa Security Program.
20 (E) The Department of Homeland Secu-
21 rity, Office of Intelligence and Analysis.
22 (F) The Federal Bureau of Investigation.
23 (G) At least two representatives from the
24 Department of State, Bureau of Consular Af-
25 fairs.

(H) Private sector and higher education personnel, as appropriate and to a degree that would not detrimentally impact any ongoing law enforcement investigation or intelligence operation, as determined by the Secretary of Homeland Security.

(4) CONSULTATION.—In carrying out the objectives described in paragraph (2), the interagency working group shall coordinate and consult regularly with the National Science, Technology, and Security Roundtable established under section 1746(b) of the National Defense Authorization Act for Fiscal Year 2020 (Public Law 116–92).

(5) REPORT.—Not later than one year after the commencement of the review required under paragraph (1), the interagency working group shall submit to the appropriate congressional committees a report—

(A) detailing the results of such review and the analyses and evaluation required under paragraph (2)(A); and

(B) identifying any legislative solutions necessary to improve the ability of the Department of Homeland Security, the Department of State, or both, to identify, investigate, and pre-

vent the illicit transfer of sensitive technologies from United States institutions of higher education and research institutions as a result of programs of study related to sensitive technologies undertaken by aliens described in subparagraph (F), (J), or (M) of section 101(a)(15) of the Immigration and Nationality Act (8 U.S.C. 1101(a)(15)).

(6) DEFINITIONS.—In this subsection:

(A) APPROPRIATE CONGRESSIONAL COMMITTEES.—The term ''appropriate congressional committees'' means the Committee on Homeland Security, the Committee on the Judiciary, the Committee on Armed Services, and the Committee on Foreign Affairs of the House of Representatives and the Committee on Homeland Security and Governmental Affairs, the Committee on the Judiciary, the Committee on Armed Services, and the Committee on Foreign Relations of the Senate.

(B) 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).

(C) PROGRAM OF STUDY.—The term ''program of study'' means any degree program, field of study, significant coursework, research, or laboratory access related to sensitive technologies, or other academic activity required to be reported pursuant to section 641(a) of the Omnibus Consolidated Appropriations Act, 1997 (Public Law 104–208 (8 U.S.C. 1372(a))).

(D) SENSITIVE TECHNOLOGIES.—The term ''sensitive technologies'' has the meaning given such term in paragraph (8) of section 428(e) of the Homeland Security Act of 2002 (6 U.S.C. 236(e)), as added by subsection (b).

(b) AMENDMENTS TO THE HOMELAND SECURITY ACT OF 2002 AND RELATED VISA SECURITY MATTERS.—

(1) PROGRAM SCOPE.—Paragraph (1) of section 428(e) of the Homeland Security Act of 2002 (6 U.S.C. 236(e)) is amended—

(A) by striking ''The Secretary'' and inserting the following:

''(A) AUTHORIZATION.—The Secretary''; and

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

1 ''(B) RISK-BASED ASSIGNMENTS.—
2 ''(i) IN GENERAL.—Assignments
3 under subparagraph (A) shall be made—
4 ''(I) in a risk-based manner;
5 ''(II) considering the criteria de-
6 scribed in clause (ii); and
7 ''(III) in accordance with Na-
8 tional Security Decision Directive 38
9 of June 2, 1982, or any superseding
10 presidential directive concerning staff-
11 ing at diplomatic and consular posts.
12 ''(ii) CRITERIA DESCRIBED.—The cri-
13 teria described in this clause are the fol-
14 lowing:
15 ''(I) The number of nationals of
16 the subject country who were identi-
17 fied in United States Government
18 databases related to the identities of
19 known or suspected terrorists during
20 the previous two years.
21 ''(II) Information on the coopera-
22 tion of such country with the counter-
23 terrorism efforts of the United States.
24 ''(III) Information analyzing the
25 presence, activity, or movement of ter-

rorist organizations (as such term is defined in section 212(a)(3)(B)(vi) of the Immigration and Nationality Act (8 U.S.C. 1182(a)(3)(B)(vi))) within or through such country.

''(IV) The number of formal objections and denials based on derogatory information issued through the interagency Security Advisory Opinion process.

''(V) Countries identified as a strategic competitor in the 'Summary of the 2018 National Defense Strategy of the United States of America: Sharpening the American Military's Competitive Edge' issued by the Department of Defense pursuant to section 113(g)(1)(A) of title 10, United States Code, or any successor document.

''(VI) The number of cases involving counterintelligence, illicit technology transfer, and counterproliferation related to the identities of nationals of such country.

"(VII) Information on the cooperation of such country with the counterintelligence, countering nontraditional collection, illicit technology transfer, and counterproliferation efforts of the United States, including information on foreign government-owned infrastructure and organizations dedicated to such matters.

"(VIII) The adequacy of the border and immigration control of such country.

"(IX) Any other criteria the Secretary determines appropriate.

"(iii) PRIORITIZATION.—The Secretary shall, until December 31, 2024, prioritize the establishment of new overseas assignments made under this subsection to diplomatic and consular posts in countries that are strategic competitors with the goal of countering the exploitation or illicit transfer of sensitive technologies by aliens described in subparagraph (F), (J), or (M) of section 101(a)(15) of such Act (8 U.S.C. 1101(a)(15)).".

(2) SCREENING.—Paragraph (2) of section 428(e) of the Homeland Security Act of 2002 (6 U.S.C. 236(e)) is amended—

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

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

''(C) Review visa applications of aliens against appropriate criminal, national security, and terrorism databases or other relevant information maintained by the Federal Government to improve the detection and examination of aliens whose entry into the United States would pose a substantial risk of the illicit transfer of sensitive technologies.''.

(3) DEFINITION.—Subsection (e) of section 428 of the Homeland Security Act of 2002 (6 U.S.C. 236(e)) is amended by inserting at the end the following new paragraph:

''(8) DEFINITION.—In this subsection, the term 'sensitive technologies' means—

''(A) areas of research or technology that require additional protection, as established by the interagency working group in accordance with section 1746(a)(3)(E)(i)(III) of the Na-

tional Defense Authorization Act for Fiscal Year 2020 (Public Law 116–92);

"(B) emerging and foundational technologies identified through the interagency process established under section 1758 of the John S. McCain National Defense Authorization Act for Fiscal Year 2019 (Public Law 115–232);

"(C) sciences, technologies, and associated programs of study at an institution of higher education, related to energy, nuclear science, nuclear engineering, or a related field for which an alien who is a citizen of Iran would be denied a visa to participate in coursework pursuant to section 501 of the Iran Threat Reduction and Syria Human Rights Act of 2012 (22 U.S.C. 8771); and

"(D) technologies and items included on the Commerce Control List, the United States Munitions List, the Nuclear Regulatory Commission Controls, or the Technology Alert List.".

(4) MEMORANDUM OF UNDERSTANDING.—Not later than 18 months days after the date of the enactment of this Act, the Secretary of Homeland Se-

curity and the Secretary of State shall jointly develop and submit to the appropriate congressional committees a memorandum of understanding detailing the responsibilities of and procedures used by Department of Homeland Security personnel assigned to diplomatic and consular posts under section 428 of the Homeland Security Act of 2002, as amended by this subsection, including visa security vetting and screening activities, the collection and distribution of relevant fees, and the sharing of information on visa refusals based on derogatory information issued through the interagency Security Advisory Opinion process.

(5) MACHINE READABLE TECHNOLOGY PILOT PROGRAM.—

(A) IN GENERAL.—Not later than one year after the date of the enactment of this Act, the Secretary of Homeland Security and the Secretary of State shall jointly commence a pilot program at a United States diplomatic or consular post in a country with a high volume of individuals who are known to have engaged in government sponsored technology transfer campaigns. The pilot program shall—

(i) be conducted for not fewer than 365 days; and

(ii) assess opportunities to enhance security vetting, including the use of machine-readable technology and applicant interviews, to better defend research or sensitive technologies in the United States from foreign government sponsored technology transfer campaigns.

(B) MACHINE READABLE TECHNOLOGY.—The Secretary of Homeland Security and the Secretary of State shall jointly, as part of the pilot program under subparagraph (A)—

(i) deploy and test equipment and technology to ensure that all documents collected in connection with visa applications are stored in a machine-readable and content-searchable format compatible and shareable between the Department of Homeland Security and the Department of State, and as appropriate, other interagency partners;

(ii) collect supplemental documents from visa applicants in accordance with the requirements under subparagraph (A), as

appropriate, and ensure appropriate personnel from the Department of Homeland Security and the Department of State have access to such documents for visa security vetting purposes; and

(iii) evaluate the use of such technology and supplemental documents in improving the efficacy and efficiency of visa security vetting.

(C) APPLICANT INTERVIEWS.—The Secretary of Homeland Security, in coordination with the Secretary of State, shall determine whether additional questions or further documentation requests may be appropriate during visa applicant in-person interviews to improve visa security vetting to address evolving threats to the United States.

(D) REPORT.—Not later than 420 days after the initiation of the pilot program under subparagraph (A), the Secretary of Homeland Security and the Secretary of State shall jointly submit to the appropriate congressional committees and other appropriate Federal partners a report on the following:

(i) The results of the pilot program.

(ii) Recommendations for machine-readable and content searchable equipment and technology and supplemental documents under paragraph (2).

(iii) Recommendations for additional interview questions and further documentation requests under paragraph (3).

(iv) A determination as to whether and where to expand the use of technologies evaluated during the pilot program.

(6) DEFINITIONS.—In this subsection:

(A) APPROPRIATE CONGRESSIONAL COMMITTEES.—The term ''appropriate congressional committees'' means—

(i) the Committee on Homeland Security and the Committee on Foreign Affairs of the House of Representatives; and

(ii) the Committee on Homeland Security and Governmental Affairs and the Committee on Foreign Relations of the Senate.

(B) SCREENING.—The term ''screening'' means the review of public, private, or governmental information to assess the accuracy and

1 authenticity of claims made on a visa applica-
2 tion, including information contained in Federal
3 Government records to include derogatory infor-
4 mation.

5 (C) SENSITIVE TECHNOLOGIES.—The term
6 ''sensitive technologies'' has the meaning given
7 such term in paragraph (8) of section 428(e) of
8 the Homeland Security Act of 2002 (6 U.S.C.
9 236(e)), as added by subsection (a)

10 (D) STRATEGIC COMPETITOR.—The term
11 ''strategic competitor'' means a country identi-
12 fied as a strategic competitor to the United
13 States in the ''Summary of the 2018 National
14 Defense Strategy of the United States of Amer-
15 ica: Sharpening the American Military's Com-
16 petitive Edge'' issued by the Department of De-
17 fense pursuant to section 113(g)(1)(A) of title
18 10, United States Code, or any successor docu-
19 ment.

20 (E) VETTING.—The term ''vetting'' with
21 respect to a visa applicant means the review
22 and use of information collected during screen-
23 ing, any additional information obtained
24 through interviews, consultation with other
25 Federal Government officials, derogatory infor-

mation, and information drawn from other sources to reach a determination regarding a national security concern related to the visa applicant.

SEC. 208. CHEMICAL, BIOLOGICAL, RADIOLOGICAL, AND NUCLEAR INTELLIGENCE AND INFORMATION SHARING.

(a) IN GENERAL.—Subtitle A of title II of the Homeland Security Act of 2002 (6 U.S.C. 121 et seq.), as amended by this title, is further amended by adding at the end the following new section:

"SEC. 210J. CHEMICAL, BIOLOGICAL, RADIOLOGICAL, AND NUCLEAR INTELLIGENCE AND INFORMATION SHARING.

"(a) IN GENERAL.—The Office of Intelligence and Analysis, in consultation with the Director of the Countering Weapons of Mass Destruction Office, of the Department of Homeland Security shall—

"(1) support homeland security-focused intelligence analysis of terrorist actors, their claims, and their plans to conduct attacks involving chemical, biological, radiological, or nuclear materials against the United States, including critical infrastructure;

1 ''(2) support homeland security-focused intel-
2 ligence analysis of global infectious disease, public
3 health, food, agricultural, and veterinary issues;
4 ''(3) support homeland security-focused risk
5 analysis and risk assessments of the homeland secu-
6 rity hazards described in paragraphs (1) and (2), in-
7 cluding the storage and transportation of chemical,
8 biological, nuclear, and radiological materials, by
9 providing relevant quantitative and nonquantitative
10 threat information;
11 ''(4) leverage existing and emerging homeland
12 security intelligence capabilities and structures to
13 enhance early detection, prevention, protection, re-
14 sponse, and recovery efforts with respect to a chem-
15 ical, biological, radiological, or nuclear attack;
16 ''(5) share information and provide tailored an-
17 alytical support on such threats to State, local, Trib-
18 al, and territorial authorities, and other Federal
19 agencies, as well as relevant national biosecurity and
20 biodefense stakeholders, as appropriate; and
21 ''(6) perform other responsibilities, as assigned
22 by the Secretary.
23 ''(b) COORDINATION.—Where appropriate, the Office
24 of Intelligence and Analysis shall coordinate with other
25 relevant Department components, agencies within the in-

1 telligence community, including the National Counter Pro-
2 liferation Center, and other Federal, State, local, Tribal,
3 and territorial authorities, including officials from high-
4 threat urban areas, State and major urban area fusion
5 centers, and local public health departments, as appro-
6 priate, and enable such entities to provide recommenda-
7 tions on optimal information sharing mechanisms, includ-
8 ing expeditious sharing of classified information, and on
9 how such entities can provide information to the Depart-
10 ment.

11 ''(c) DEFINITIONS.—In this section:

12 ''(1) INTELLIGENCE COMMUNITY.—The term
13 'intelligence community' has the meaning given such
14 term in section 3(4) of the National Security Act of
15 1947 (50 U.S.C. 3003(4)).

16 ''(2) NATIONAL BIOSECURITY AND BIODEFENSE
17 STAKEHOLDERS.—The term 'national biosecurity
18 and biodefense stakeholders' means officials from
19 Federal, State, local, Tribal, and territorial authori-
20 ties and individuals from the private sector who are
21 involved in efforts to prevent, protect against, re-
22 spond to, and recover from a biological attack or
23 other phenomena that may have serious health con-
24 sequences for the United States, including infectious
25 disease outbreaks.''.

(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 201I, as added by this title, the following new item:

"Sec. 210J. Chemical, biological, radiological, and nuclear intelligence and information sharing.".

(c) REPORT.—

(1) IN GENERAL.—Not later than one year after the date of the enactment of this Act and annually thereafter for each of the following four years, the Secretary of Homeland Security shall report to the appropriate congressional committees on the following:

(A) The intelligence and information sharing activities under section 210J of the Homeland Security Act of 2002 (as added by subsection (a) of this section) and of all relevant entities within the Department of Homeland Security to counter the threat from attacks using chemical, biological, radiological, or nuclear materials.

(B) The Department's activities in accordance with relevant intelligence strategies.

(2) ASSESSMENT OF IMPLEMENTATION.—The reports required under paragraph (1) shall include the following:

(A) An assessment of the progress of the Office of Intelligence and Analysis of the Department of Homeland Security in implementing such section 210J.

(B) A description of the methods established to carry out such assessment.

(3) DEFINITION.—In this subsection, the term ''appropriate congressional committees'' means the Committee on Homeland Security of the House of Representatives and the Committee on Homeland Security and Governmental Affairs of the Senate and any committee of the House of Representatives or the Senate having legislative jurisdiction under the rules of the House of Representatives or Senate, respectively, over the matter concerned.

SEC. 209. INLAND WATERS THREAT ANALYSIS.

(a) IN GENERAL.—Not later than 180 days after the date of the enactment of this Act, the Secretary of Homeland Security shall submit to the appropriate congressional committees an inland waters threat analysis that includes an identification and description of the following:

(1) Current and potential terrorism and criminal threats posed by individuals and groups seeking to—

(A) enter the United States through inland waters; or

(B) exploit security vulnerabilities on inland waters.

(2) Security challenges at United States inland waters ports regarding—

(A) terrorism and instruments of terror entering the United States; and

(B) criminal activity, as measured by the total flow of illegal goods and illicit drugs, related to the inland waters.

(3) Security mitigation efforts with respect to the inland waters to—

(A) prevent terrorists and instruments of terror from entering the United States; and

(B) reduce criminal activity related to the inland waters.

(4) Vulnerabilities related to cooperation between State, local, Tribal, and territorial law enforcement, or international agreements, that hinder effective security, counterterrorism, anti-trafficking efforts, and the flow of legitimate trade with respect to inland waters.

(5) Metrics and performance measures used by the Department of Homeland Security to evaluate inland waters security, as appropriate.

(b) ANALYSIS REQUIREMENTS.—In preparing the threat analysis required under subsection (a), the Secretary of Homeland Security shall consider and examine the following:

(1) Technology needs and challenges.

(2) Personnel needs and challenges.

(3) The roles of State, local, Tribal, and territorial law enforcement, as well as private sector partners and the public, relating to inland waters security.

(4) The need for cooperation among Federal, State, local, Tribal, territorial, and international partner law enforcement, as well as private sector partners and the public, relating to inland waters security.

(5) The challenges posed by geography with respect to inland waters security.

(c) CLASSIFIED THREAT ANALYSIS.—To the extent possible, the Secretary of Homeland Security shall submit the threat analysis required under subsection (a) in unclassified form. The Secretary may submit a portion of

the threat analysis in classified form if the Secretary determines that such is appropriate.

(d) DEFINITIONS.—In this section:

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

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

(B) the Committee on Homeland Security and Government Affairs of the Senate; and

(C) the Committee on Commerce, Science, and Transportation of the Senate.

(2) The term ''inland waters'' has the meaning given such term in section 83.03 of title 33, Code of Federal Regulations.

SEC. 210. TRANSNATIONAL CRIMINAL ORGANIZATIONS THREAT ASSESSMENT.

(a) IN GENERAL.—Not later than 90 days after the date of the enactment of this Act, the Under Secretary for Intelligence and Analysis shall, in coordination with appropriate Federal partners, develop and disseminate a threat assessment on whether transnational criminal organizations are exploiting United States border security vulnerabilities in border security screening programs to gain access to the United States and threaten the United States or border security.

(b) RECOMMENDATIONS.—Upon completion of the threat assessment required under subsection (a), the Secretary of Homeland Security shall make a determination if any changes are required to address security vulnerabilities identified in such assessment.

(c) DISTRIBUTION.—Consistent with the protection of classified and confidential unclassified information, the Under Secretary for Intelligence and Analysis shall share the threat assessment developed under this section with State, local, and Tribal law enforcement officials, including officials that operate within fusion centers in the National Network of Fusion Centers.

SEC. 211. DEPARTMENT OF HOMELAND SECURITY COUNTERTERRORISM ADVISORY BOARD.

(a) IN GENERAL.—Subtitle A of title II of the Homeland Security Act of 2002 (6 U.S.C. 121 et seq.), as amended by this title, is further amended by adding at the end the following new section:

"SEC. 210K. DEPARTMENTAL COORDINATION ON COUNTERTERRORISM.

''(a) ESTABLISHMENT.—There is in the Department a board to be composed of senior representatives of departmental operational components and headquarters elements. The purpose of the board shall be to coordinate and integrate departmental intelligence, activities, and

policy related to the counterterrorism mission and functions of the Department.

"(b) CHARTER.—There shall be a charter to govern the structure and mission of the board. Such charter shall direct the board to focus on the current threat environment and the importance of aligning departmental counterterrorism activities under the Secretary's guidance. The charter shall be reviewed and updated every 4 years, as appropriate.

"(c) MEMBERS.—

"(1) CHAIR.—The Secretary shall appoint a Coordinator for Counterterrorism within the Department who will serve as the chair of the board.

"(2) ADDITIONAL MEMBERS.—The Secretary shall appoint additional members of the board from among the following:

"(A) The Transportation Security Administration.

"(B) United States Customs and Border Protection.

"(C) United States Immigration and Customs Enforcement.

"(D) The Federal Emergency Management Agency.

"(E) The Coast Guard.

1 "(F) United States Citizenship and Immi-
2 gration Services.
3 "(G) The United States Secret Service.
4 "(H) The Cybersecurity and Infrastructure
5 Security Agency.
6 "(I) The Office of Operations Coordina-
7 tion.
8 "(J) The Office of the General Counsel.
9 "(K) The Office of Intelligence and Anal-
10 ysis.
11 "(L) The Office of Policy.
12 "(M) The Science and Technology Direc-
13 torate.
14 "(N) Other Departmental offices and pro-
15 grams as determined appropriate by the Sec-
16 retary.
17 "(d) MEETINGS.—The board shall meet on a regular
18 basis to discuss intelligence and coordinate ongoing threat
19 mitigation efforts and departmental activities, including
20 coordination with other Federal, State, local, Tribal, terri-
21 torial, and private sector partners, and shall make rec-
22 ommendations to the Secretary.
23 "(e) TERRORISM ALERTS.—The board shall advise
24 the Secretary on the issuance of terrorism alerts pursuant
25 to section 203 of this Act.

"(f) PROHIBITION ON ADDITIONAL FUNDS.—No additional funds are authorized to carry out this section.".

(b) CLERICAL AMENDMENT.—The table of contents in section 1(b) of such Act is amended by inserting after the item relating to section 210J, as added by this title, the following new item:

"Sec. 210K. Departmental coordination on counterterrorism.".

(c) REPORT.—Not later than 90 days after the date of the enactment of this Act, the Secretary, acting through the Coordinator for Counterterrorism, 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 status and activities of the board established under section 210K of the Homeland Security Act of 2002, as added by subsection (a).

SEC. 212. NATIONAL VETTING CENTER.

(a) AUTHORIZATION.—The Secretary of Homeland Security, in coordination with the Secretary of State, the Secretary of Defense, the Attorney General, and the Director of National Intelligence, shall establish and operate a National Vetting Center.

(b) DIRECTOR.—The Secretary of Homeland Security shall appoint a senior departmental employee to be the director of the center.

1 (c) STAFFING.—The Secretary of Homeland Security
2 shall—
3 (1) assign or detail appropriate personnel from
4 the department to serve as analysts at the National
5 Vetting Center; and
6 (2) coordinate with the Director of National In-
7 telligence and the heads of other appropriate Fed-
8 eral agencies to detail appropriate personnel to serve
9 as analysts at the National Vetting Center.
10 (d) PURPOSE.—The National Vetting Center shall,
11 consistent with the guidance and oversight from the Na-
12 tional Vetting Governance Board established pursuant to
13 section 214 of this Act—
14 (1) coordinate the efforts of Federal agencies to
15 improve vetting of individuals seeking to enter or re-
16 main within the United States;
17 (2) assist the departments and agencies in-
18 volved with improving their coordination and use of
19 intelligence and other information to identify poten-
20 tial threats to national security, border security,
21 homeland security, and public safety;
22 (3) provide a forum for the departments and
23 agencies involved to identify, coordinate, and resolve
24 policy questions and implementation challenges asso-
25 ciated with vetting;

(4) improve the effectiveness of vetting operations by maximizing the Intelligence Community and law enforcement data holdings used to support vetting;

(5) develop and maintain a process to ensure compliance with legal, privacy, and civil rights and civil liberty requirements; and

(6) other responsibilities as determined by the Secretary of Homeland Security.

SEC. 213. NATIONAL VETTING GOVERNANCE BOARD.

(a) ESTABLISHMENT.—The Secretary of Homeland Security, in coordination with the Secretary of State, the Secretary of Defense, the Attorney General, and the Director of National Intelligence, shall establish a National Vetting Governance Board.

(b) PURPOSE.—The National Vetting Governance Board shall provide guidance and oversight for the National Vetting Center established pursuant to section 213 of this Act, including—

(1) producing decisions and recommendations for unified approaches to and solutions for vetting;

(2) recommending a fiscal strategy;

(3) recommending priorities for National Vetting Center activities;

(4) reviewing and recommending new vetting programs or changes to existing vetting activities;

(5) reporting progress and making recommendations to Secretary of Homeland Security or their designee; and

(6) ensuring National Vetting Governance Board decisions and recommendations are consistent with relevant legal authorities and align with Department of Homeland Security privacy, civil rights, and civil liberties policies and practices.

(c) LIMITATIONS.—The National Vetting Governance Board is not intended to supersede or otherwise replace existing statutory or delegated roles and responsibilities concerning Department of Homeland Security vetting activities.

(d) OPERATIONS.—

(1) The Secretary of Homeland Security, in coordination with the Secretary of State, the Secretary of Defense, the Attorney General, and the Director of National Intelligence shall develop the structure, staffing, meeting schedule and other operational issues related to the National Vetting Governance Board.

(2) The National Vetting Governance Board shall have a standing privacy and civil liberty work-

ing group and a legal working group to review the activities of the National Vetting Center and provide advice to the Board.

Subtitle B—Information Sharing

SEC. 215. DEPARTMENT OF HOMELAND SECURITY FUSION CENTER PARTNERSHIP INITIATIVE.

(a) IN GENERAL.—Section 210A of the Homeland Security Act of 2002 (6 U.S.C. 124h) is amended—

(1) by amending the section heading to read as follows:

"SEC. 210A. DEPARTMENT OF HOMELAND SECURITY FUSION CENTER PARTNERSHIP INITIATIVE.";

(2) in subsection (a), by adding at the end the following: ''Beginning on the date of enactment of the Department of Homeland Security Authorization Act, such Initiative shall be known as the 'Department of Homeland Security Fusion Center Partnership Initiative'.'';

(3) by amending subsection (b) to read as follows:

''(b) INTERAGENCY SUPPORT AND COORDINATION.—Through the Department of Homeland Security Fusion Center Partnership Initiative, in coordination with principal officials of fusion centers in the National Network of Fusion Centers and the officers designated as the

1 Homeland Security Advisors of the States, the Secretary
2 shall—
3 ''(1) coordinate with the heads of other Federal
4 departments and agencies to provide operational,
5 analytic, and reporting intelligence advice and assist-
6 ance to the National Network of Fusion Centers and
7 to align homeland security intelligence activities with
8 other field based intelligence activities;
9 ''(2) support the integration of fusion centers
10 into the information sharing environment, including
11 by—
12 ''(A) providing for the effective dissemina-
13 tion of information within the scope of the in-
14 formation sharing environment to the National
15 Network of Fusion Centers;
16 ''(B) conducting outreach to such fusion
17 centers to identify any gaps in information
18 sharing;
19 ''(C) consulting with other Federal agen-
20 cies to develop methods to—
21 ''(i) address any such gaps identified
22 under subparagraph (B), as appropriate;
23 and
24 ''(ii) deploy or access such databases
25 and datasets, as appropriate; and

1 ''(D) review information that is gathered
2 by the National Network of Fusion Centers to
3 identify that which is within the scope of the in-
4 formation sharing environment, including home-
5 land security information (as defined in section
6 892), terrorism information, and weapons of
7 mass destruction information and incorporate
8 such information, as appropriate, into the De-
9 partment's own such information;
10 ''(3) facilitate close communication and coordi-
11 nation between the National Network of Fusion
12 Centers and the Department and other Federal de-
13 partments and agencies;
14 ''(4) facilitate information sharing and expertise
15 from the national cybersecurity and communications
16 integration center under section 2209 to the Na-
17 tional Network of Fusion Centers;
18 ''(5) coordinate the provision of training and
19 technical assistance, including training on the use of
20 Federal databases and datasets described in para-
21 graph (2), to the National Network of Fusion Cen-
22 ters and encourage participating fusion centers to
23 take part in terrorism threat-related exercises con-
24 ducted by the Department;

1 ''(6) ensure the dissemination of cyber threat
2 indicators and information about cybersecurity risks
3 and incidents to the national Network of Fusion
4 Centers;
5 ''(7) ensure that each fusion center in the Na-
6 tional Network of Fusion Centers has a privacy pol-
7 icy approved by the Chief Privacy Officer of the De-
8 partment and a civil rights and civil liberties policy
9 approved by the Officer for Civil Rights and Civil
10 Liberties of the Department;
11 ''(8) develop and disseminate best practices on
12 the appropriate levels for staffing at fusion centers
13 in the National Network of Fusion Centers of quali-
14 fied representatives from State, local, Tribal, and
15 territorial law enforcement, fire, emergency medical,
16 and emergency management services, and public
17 health disciplines, as well as the private sector;
18 ''(9) to the maximum extent practicable, pro-
19 vide guidance, training, and technical assistance to
20 ensure fusion centers operate in accordance with and
21 in a manner that protects privacy, civil rights, and
22 civil liberties afforded by the Constitution of the
23 United States;
24 ''(10) to the maximum extent practicable, pro-
25 vide guidance, training, and technical assistance to

ensure fusion centers are appropriately aligned with and able to meaningfully support Federal homeland security, national security, and law enforcement efforts, including counterterrorism;

''(11) encourage the full participation of the National Network of Fusion Centers in all assessment and evaluation efforts conducted by the Department;

''(12) track all Federal funding provided to each fusion center on an individualized basis as well as by funding source;

''(13) ensure that none of the departmental information or data provided or otherwise made available to fusion center personnel is improperly disseminated, accessed for unauthorized purposes, or otherwise used in a manner inconsistent with Department guidance; and

''(14) carry out such other duties as the Secretary determines appropriate.'';

(4) in subsection (c)—

(A) in the heading, by striking ''PERSONNEL ASSIGNMENT'' and inserting ''RESOURCE ALLOCATION'';

(B) by striking paragraphs (1) and (2) and inserting the following:

1 "(1) INFORMATION SHARING AND PERSONNEL
2 ASSIGNMENT.—
3 "(A) INFORMATION SHARING.—The Under
4 Secretary for Intelligence and Analysis shall en-
5 sure that, as appropriate—
6 "(i) fusion centers in the National
7 Network of Fusion Centers have access to
8 homeland security information sharing sys-
9 tems; and
10 "(ii) Department personnel are de-
11 ployed to support fusion centers in the Na-
12 tional Network of Fusion Centers in a
13 manner consistent with the mission of the
14 Department.
15 "(B) PERSONNEL ASSIGNMENT.—Depart-
16 ment personnel referred to in subparagraph
17 (A)(ii) may include the following:
18 "(i) Intelligence officers.
19 "(ii) Intelligence analysts.
20 "(iii) Other liaisons from components
21 and offices of the Department, as appro-
22 priate.
23 "(2) SOURCES OF SUPPORT.—Information
24 shared and personnel assigned pursuant to para-
25 graph (1) may be shared or provided, as the case

may be, by the following Department components and offices, in coordination with the respective component or office head and in consultation with the principal officials of fusion centers in the National Network of Fusion Centers:

"(A) The Office of Intelligence and Analysis.

"(B) Cybersecurity and Infrastructure Security Agency.

"(C) The Transportation Security Administration.

"(D) U.S. Customs and Border Protection.

"(E) U.S. Immigration and Customs Enforcement.

"(F) The Coast Guard.

"(G) The national cybersecurity and communications integration center under section 2209.

"(H) Other components or offices of the Department, as determined by the Secretary.";

(C) in paragraph (3)—

(i) in the heading, by striking "QUALIFYING CRITERIA" and inserting "RESOURCE ALLOCATION CRITERIA"; and

(ii) by striking subparagraph (A) and inserting the following:

''(A) IN GENERAL.—The Secretary shall make available criteria for sharing information and deploying personnel to support a fusion center in the National Network of Fusion Centers in a manner consistent with the Department's mission and existing statutory limits.''; and

(D) in paragraph (4)(B), in the matter preceding clause (i), by inserting ''in which such fusion center is located'' after ''region'';

(5) in subsection (d)—

(A) in paragraph (3), by striking ''and'' at the end;

(B) by redesignating paragraph (4) as paragraph (5);

(C) by inserting after paragraph (3) the following:

''(4) assist, in coordination with the national cybersecurity and communications integration center under section 2209, fusion centers in using information relating to cybersecurity risks to develop a comprehensive and accurate threat picture;'';

(D) in paragraph (5), as so redesignated—

(i) by striking ''government'' and inserting ''governments''; and

(ii) by striking the period at the end and inserting ''; and''; and

(E) by adding at the end the following:

''(6) use Department information, including information held by components and offices, to develop analysis focused on the mission of the Department under section 101(b).'';

(6) in subsection (e)—

(A) by amending paragraph (1) to read as follows:

''(1) IN GENERAL.—To the greatest extent practicable, the Secretary shall make it a priority to allocate resources, including departmental component personnel with relevant expertise, to support the efforts of fusion centers along land or maritime borders of the United States to facilitate law enforcement agency identification, investigation, and interdiction of persons, weapons, and related contraband that pose a threat to homeland security.''; and

(B) in paragraph (2), in the matter preceding subparagraph (A), by striking ''participating State, local, and regional fusion centers''

and inserting ''fusion centers in the National Network of Fusion Centers'';

(7) in subsection (j)—

(A) by redesignating paragraph (5) as paragraph (7);

(B) by redesignating paragraphs (1) through (4) as paragraphs (2) through (5), respectively;

(C) by inserting before paragraph (2) the following:

''(1) the term 'cybersecurity risk' has the meaning given such term in section 2209;'';

(D) in paragraph (5), as so redesignated, by striking ''and'' at the end; and

(E) by inserting after such paragraph (5) the following new paragraph:

''(6) the term 'National Network of Fusion Centers' means a decentralized arrangement of fusion centers intended to enhance individual State and urban area fusion centers' ability to leverage the capabilities and expertise of all fusion centers for the purpose of enhancing analysis and homeland security information sharing nationally; and''; and

(8) by striking subsection (k).

(b) REPORT.—Not later than 1 year after the date of the enactment of this Act and annually thereafter through 2024, the Under Secretary for Intelligence and Analysis of the Department of Homeland Security shall report to the Committee on Homeland Security and the Permanent Select Committee on Intelligence of the House of Representatives and the Committee on Homeland Security and Governmental Affairs and the Select Committee on Intelligence of the Senate on the value of fusion center intelligence products and the expenditure of authorized funds for the support and coordination of the National Network of Fusion Centers as specified in section 210A of the Homeland Security Act of 2002 (6 U.S.C. 124h), as amended by subsection (a).

(c) REPORT ON FEDERAL DATABASES.—Not later than 180 days after the date of enactment of this Act, the Comptroller General of the United States shall submit a report to Congress on the Federal databases and datasets that address any gaps identified pursuant to section 210A(b)(2)(B) of the Homeland Security Act of 2002, as amended by subsection (a), including databases and datasets used, operated, or managed by Department components, the Department of Justice, including the Federal Bureau of Investigation and the Drug Enforcement Administration, and the Department of the Treas-

ury, that are appropriate, in accordance with Federal laws and policies, for inclusion in the information sharing environment.

(d) TECHNICAL AND CONFORMING AMENDMENTS.—

(1) Section 2103(c)(1) of the Homeland Security Act of 2002 (6 U.S.C. 623(c)(1)) is amended by striking "210A(j)(1)" and inserting "210A(j)".

(2) The table of contents in section 1(b) of the Homeland Security Act of 2002 is amended by striking the item relating to section 210A and inserting the following:

"Sec. 210A. Department of Homeland Security Fusion Center Partnership Initiative.".

(e) REFERENCE.—Any reference in any law, rule, or regulation to the Department of Homeland Security State, Local, and Regional Fusion Center Initiative shall be deemed to be a reference to the Department of Homeland Security Fusion Center Partnership Initiative.

SEC. 216. FUSION CENTER PERSONNEL NEEDS ASSESSMENT.

(a) ASSESSMENT.—

(1) IN GENERAL.—Not later than 240 days after the date of the enactment of this Act, the Comptroller General of the United States shall conduct an assessment of Department of Homeland Security personnel assigned to fusion centers pursuant

to section 210A(c) of the Homeland Security Act of 2002 (6 U.S.C. 124h(c)), as amended by this title, including an assessment of whether deploying additional Department personnel to such fusion centers would enhance the Department's mission under section 101(b) of such Act (6 U.S.C. 111(b)) and the National Network of Fusion Centers.

(2) CONTENTS.—The assessment required under this subsection shall include the following:

(A) Information on the current deployment of the Department's personnel to each fusion center.

(B) Information on the roles and responsibilities of the Department's Office of Intelligence and Analysis intelligence officers, intelligence analysts, senior reports officers, reports officers, and regional directors deployed to fusion centers.

(C) Information on Federal resources, in addition to personnel, provided to each fusion center.

(D) An analysis of the optimal number of personnel the Office of Intelligence and Analysis should deploy to fusion centers, including a cost-benefit analysis comparing deployed per-

sonnel with technological solutions to support information sharing.

(E) An assessment of fusion centers located in jurisdictions along land and maritime borders of the United States, and the degree to which deploying personnel, as appropriate, from U.S. Customs and Border Protection, U.S. Immigration and Customs Enforcement, and the Coast Guard to such fusion centers would enhance the integrity and security at such borders by helping Federal, State, local, Tribal, and territorial law enforcement authorities to identify, investigate, and interdict persons, weapons, and related contraband that pose a threat to homeland security.

(F) An assessment of fusion centers located in jurisdictions with large and medium hub airports, and the degree to which deploying, as appropriate, personnel from the Transportation Security Administration to such fusion centers would enhance the integrity and security of aviation security.

(b) DEFINITIONS.—In this section, the terms ''fusion center'' and ''National Network of Fusion Centers'' have the meanings given those terms in section 210A(j) of the

1 Homeland Security Act of 2002 (6 U.S.C. 124h(j)), as
2 amended by this title.

3 **SEC. 217. PROGRAM FOR STATE AND LOCAL ANALYST**
4 **CLEARANCES.**

5 (a) SENSE OF CONGRESS.—It is the sense of Con-
6 gress that any program established by the Under Sec-
7 retary for Intelligence and Analysis of the Department of
8 Homeland Security to provide eligibility for access to in-
9 formation classified as Top Secret for State, local, Tribal,
10 and territorial analysts located in fusion centers shall be
11 consistent with the need to know requirements pursuant
12 to Executive Order No. 13526 (50 U.S.C. 3161 note).

13 (b) REPORT.—Not later than two years after the date
14 of the enactment of this Act, the Under Secretary for In-
15 telligence and Analysis of the Department of Homeland
16 Security, in consultation with the Director of National In-
17 telligence, shall submit to the Committee on Homeland Se-
18 curity and the Permanent Select Committee on Intel-
19 ligence of the House of Representatives and the Com-
20 mittee on Homeland Security and Governmental Affairs
21 and the Select Committee on Intelligence of the Senate
22 a report on the following:

23 (1) The process by which the Under Secretary
24 for Intelligence and Analysis determines a need to
25 know pursuant to Executive Order No. 13526 (50

U.S.C. 3161 note) to sponsor Top Secret clearances for appropriate State, local, Tribal, and territorial analysts located in fusion centers.

(2) The effects of such Top Secret clearances on enhancing information sharing with State, local, Tribal, and territorial partners.

(3) The cost for providing such Top Secret clearances for State, local, Tribal, and territorial analysts located in fusion centers, including training and background investigations.

(4) The operational security protocols, training, management, and risks associated with providing such Top Secret clearances for State, local, Tribal, and territorial analysts located in fusion centers.

(c) DEFINITION.—In this section, the term ''fusion center'' has the meaning given the term in section 210A(j) of the Homeland Security Act of 2002 (6 U.S.C. 124h(j)), as amended by this title.

SEC. 218. INFORMATION TECHNOLOGY ASSESSMENT.

(a) IN GENERAL.—The Under Secretary for Intelligence and Analysis of the Department of Homeland Security, in collaboration with the Chief Information Officer of the Department of Homeland Security and representatives from the National Network of Fusion Centers, shall conduct an assessment of information systems used to

share homeland security information between the Department of Homeland Security and fusion centers in the National Network of Fusion Centers and make upgrades to such systems, as appropriate. Such assessment shall include the following:

(1) An evaluation of the security, accessibility, and ease of use of such systems by fusion centers in the National Network of Fusion Centers.

(2) A review to determine how to establish improved interoperability of departmental information systems with existing information systems used by fusion centers in the National Network of Fusion Centers.

(3) An evaluation of participation levels of departmental components and offices of information systems used to share homeland security information with fusion centers in the National Network of Fusion Centers.

(b) DEFINITIONS.—In this section—

(1) the terms ''fusion center'' and ''National Network of Fusion Centers'' have the meanings given those terms in section 210A(j) of the Homeland Security Act of 2002 (6 U.S.C. 124h(j)), as amended by this title;

(2) the term ''homeland security information'' has the meaning given the term in section 892 of the Homeland Security Act of 2002 (6 U.S.C. 482); and

(3) the term ''information systems'' has the meaning given the term in section 3502 of title 44, United States Code.

SEC. 219. DEPARTMENT OF HOMELAND SECURITY CLASSIFIED FACILITY INVENTORY AND DISSEMINATION.

(a) IN GENERAL.—The Secretary of Homeland Security shall, to the extent practicable—

(1) maintain an inventory of those Department of Homeland Security facilities that the Department certifies to house classified infrastructure or systems at the Secret level and above;

(2) update such inventory on a regular basis; and

(3) share part or all of such inventory with appropriate departmental personnel and representatives of other Federal, State, and local agencies as determined appropriate by the Secretary of Homeland Security.

(b) INVENTORY.—The inventory of facilities described in subsection (a) may include—

(1) the location of such facilities;

(2) the attributes and capabilities of such facilities (including the clearance level of the facility, the square footage of, the total capacity of, the number of workstations in, document storage, and the number of conference rooms in, such facilities);

(3) the entities that operate such facilities; and

(4) the date of establishment of such facilities.

SEC. 220. TERROR INMATE INFORMATION SHARING.

(a) IN GENERAL.—The Secretary of Homeland Security, in coordination with the Attorney General and in consultation with other appropriate Federal officials, shall, as appropriate, share with State, local, and regional fusion centers through the Department of Homeland Security Fusion Center Partnership Initiative under section 210A of the Homeland Security Act of 2002 (6 U.S.C. 124h), as well as other relevant law enforcement entities, release information from a Federal correctional facility, including the name, charging date, and expected place and date of release, of certain individuals who may pose a terrorist threat.

(b) SCOPE.—The information shared pursuant to subsection (a) shall be—

(1) for homeland security purposes; and

(2) regarding individuals convicted of a Federal crime related to acts of terrorism (as such term is

1 defined in section 3077 of title 18, United States
2 Code).

3 (c) PERIODIC THREAT ASSESSMENTS.—Consistent
4 with the protection of classified information and controlled
5 unclassified information, the Secretary of Homeland Secu-
6 rity shall coordinate with appropriate Federal officials to
7 provide State, local, and regional fusion centers described
8 in subsection (a) with periodic assessments regarding the
9 overall threat from known or suspected terrorists currently
10 incarcerated in a Federal correctional facility, including
11 the assessed risks of such populations engaging in ter-
12 rorist activity upon release.

13 (d) PRIVACY PROTECTION.—Prior to affecting the in-
14 formation sharing described in subsection (a), the Sec-
15 retary shall receive input and advice from the Officer for
16 Civil Rights and Civil Liberties, the Officer for Privacy,
17 and the Chief Intelligence Officer of the Department of
18 Homeland Security.

19 (e) RULE OF CONSTRUCTION.—Nothing in this sec-
20 tion may be construed as requiring the establishment of
21 a list or registry of individuals convicted of terrorism.

SEC. 221. ENHANCING DEPARTMENT OF HOMELAND SECURITY SUSPICIOUS ACTIVITY REPORTING OPERATIONS.

(a) STRATEGY REQUIRED.—Not later than one year after the date of the enactment of this Act, the Secretary of Homeland Security, in consultation with other appropriate officials, shall develop a strategy to improve the operations and activities of the Department of Homeland Security related to training, outreach, and information sharing for suspicious activity reporting to prevent acts of terrorism and acts of targeted violence.

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

(1) A plan to maintain and expand activities related to effectively identifying, reporting, and responding to potential acts of terrorism.

(2) A plan to develop a behavioral threat assessment and management model for use by appropriate National Network of Fusion Centers, emergency response providers, and appropriate private sector personnel involved in reporting or responding suspicious activity related to acts of targeted violence.

(3) Protocols, developed in consultation with the Federal Bureau of Investigation, to ensure that

the Federal Bureau of Investigations receives all relevant suspicious activity reports.

(4) A staffing and budget plan to ensure the continued operation and any necessary expansion of Department of Homeland Security information sharing, technical assistance, training, and other activities related to suspicious activity reporting.

(5) Training for appropriate personnel of the National Network of Fusion Centers, emergency response providers, and appropriate private sector personnel on—

(A) methods for identifying, analyzing, and disseminating critical information, including the indicators of acts of terrorism and acts of targeted violence;

(B) methods to protect privacy and civil liberties, including preventing racial, religious, and national origin discrimination;

(C) implementation of the behavioral threat assessment and management model;

(D) response protocols for submitting suspicious activity reports; and

(E) other training determined appropriate by the Secretary.

(6) A plan to—

(A) provide technical assistance for appropriate National Network of Fusion Centers, emergency response providers, and appropriate private sector personnel for operations related to suspicious activity reporting activity; and

(B) assist with questions or concerns related to privacy and civil liberty protections.

(c) CONGRESSIONAL NOTIFICATION.—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 a copy of the strategy required in subsection (a).

(d) DEFINITIONS.—In this section:

(1) BEHAVIORAL THREAT ASSESSMENT.—The term ''behavioral threat assessment and management'' means the systematic and evidence-based process of—

(A) identifying individuals who are exhibiting patterns of concerning behavior that indicate an interest, motive, intention, or capability of carrying out an act of violence;

(B) investigating and gathering information from multiple sources to assess whether an individual described in subparagraph (A) poses a threat, based on articulable facts; and

(C) the subsequent management of such a threat, if necessary.

(2) EMERGENCY RESPONSE PROVIDERS.—The term ''emergency response provider'' has the meaning given such term in section 2(6) of the Homeland Security Act.

(3) NATIONAL NETWORK OF FUSION CENTERS.—The term ''National Network of Fusion Centers'' has the meaning given such term in section 215 of this Act.

(4) TARGETED VIOLENCE.—The term ''targeted violence'' means any incident of predatory violence with respect to which an identifiable individual or group focuses an attack on a particular target.

(5) TERRORISM.—The term ''terrorism'' has the meaning given such term in section 2331 of title 18, United States Code.

TITLE III—CYBERSECURITY

SEC. 301. CYBERSECURITY ADVISORY COMMITTEE.

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

"SEC. 2215. CYBERSECURITY ADVISORY COMMITTEE.

"(a) ESTABLISHMENT.—The Secretary shall establish within the Cybersecurity and Infrastructure Security Agency a Cybersecurity Advisory Committee.

"(b) DUTIES.—

"(1) IN GENERAL.—The Advisory Committee may advise, consult with, report to, and make recommendations to the Director of Cybersecurity and Infrastructure Security on the development, refinement, and implementation of policies, programs, rulemakings, planning, training, and security directives pertaining to the mission of the Cybersecurity and Infrastructure Security Agency.

"(2) RECOMMENDATIONS.—

"(A) IN GENERAL.—The Advisory Committee shall develop, at the request of the Director, recommendations for improvements to the cybersecurity mission of the Cybersecurity and Infrastructure Security Agency.

"(B) RECOMMENDATIONS OF SUBCOMMITTEES.—Recommendations agreed upon by the subcommittees established under subsection (d) for any year shall be approved by the Advisory Committee before the Advisory Committee submits to the Director the annual report under paragraph (4) for that year.

"(3) PERIODIC REPORTS.—The Advisory Committee shall periodically submit to the Director—

"(A) reports on matters identified by the Director; and

"(B) reports on other matters identified by a majority of the members of the Advisory Committee.

"(4) ANNUAL REPORT.—The Advisory Committee shall submit to the Director an annual report providing information on the activities, findings, and recommendations of the Advisory Committee, including its subcommittees, for the preceding year. Not later than six months after the date that the Director receives an annual report for a year, the Director shall publish a public version of the report describing the activities of the Advisory Committee and such related matters as would be informative to the public during that year, consistent with section 552(b) of title 5, United States Code.

"(5) FEEDBACK.—Not later than 90 days after receiving any recommendation submitted by the Advisory Committee under paragraph (2), (3), or (4), the Director shall respond in writing to the Advisory Committee with feedback on the recommendation. Such a response shall include—

"(A) with respect to any recommendation with which the Director concurs, an action plan to implement the recommendation; and

"(B) with respect to any recommendation with which the Director does not concur, a justification for why the Director does not plan to implement the recommendation.

"(6) CONGRESSIONAL NOTIFICATION.—For each fiscal quarter beginning after the date of the enactment of this section, the Director shall provide to the Committee on Homeland Security and Governmental Affairs and the Committee on Appropriations of the Senate and the Committee on Homeland Security and the Committee on Appropriations of the House of Representatives a briefing on feedback from the Advisory Committee.

"(c) MEMBERSHIP.—

"(1) APPOINTMENT.—

"(A) IN GENERAL.—Not later than 180 days after the date of the enactment of this Act, the Director shall appoint the members of the Advisory Committee.

"(B) COMPOSITION.—The membership of the Advisory Committee shall consist of not more than 35 individuals, each of whom rep-

1 resent a category referred to in subparagraph
2 (C)(i).
3 "(C) REPRESENTATION.—
4 "(i) IN GENERAL.—The membership
5 of the Advisory Committee shall include
6 representatives of State and local govern-
7 ments and of a broad range of industries,
8 including the following:
9 "(I) Defense.
10 "(II) Education.
11 "(III) Financial services.
12 "(IV) Healthcare.
13 "(V) Manufacturing.
14 "(VI) Media and entertainment.
15 "(VII) Chemicals.
16 "(VIII) Retail.
17 "(IX) Transportation.
18 "(X) Energy.
19 "(XI) Information Technology.
20 "(XII) Communications.
21 "(XIII) Other relevant fields
22 identified by the Director.
23 "(ii) PROHIBITION.—Not more than
24 three members may represent any one cat-
25 egory under clause (i).

1 "(2) TERM OF OFFICE.—
2 "(A) TERMS.—The term of each member
3 of the Advisory Committee shall be two years,
4 but a member may continue to serve until a
5 successor is appointed.
6 "(B) REMOVAL.—The Director may review
7 the participation of a member of the Advisory
8 Committee and remove such member for cause
9 at any time.
10 "(C) REAPPOINTMENT.—A member of the
11 Advisory Committee may be reappointed for an
12 unlimited number of terms.
13 "(3) DELEGATION OF RESPONSIBILITIES.—A
14 member of the Advisory Committee may delegate
15 that member's responsibilities under this section to
16 another individual, with the exception of access to
17 protected information and classified information
18 under paragraph (6).
19 "(4) PROHIBITION ON COMPENSATION.—The
20 members of the Advisory Committee may not receive
21 pay or benefits from the United States Government
22 by reason of their service on the Advisory Com-
23 mittee.
24 "(5) MEETINGS.—

"(A) IN GENERAL.—The Director shall require the Advisory Committee to meet at least quarterly, and may convene additional meetings as necessary.

"(B) PUBLIC MEETINGS.—At least one of the meetings referred to in subparagraph (A) shall be open to the public.

"(C) ATTENDANCE.—The Advisory Committee shall maintain a record of the persons present at each meeting.

"(6) MEMBER ACCESS TO CLASSIFIED AND PROTECTED INFORMATION.—

"(A) IN GENERAL.—Not later than 60 days after the date on which a member is first appointed to the Advisory Committee and before the member is granted access to any classified information or protected information, the Director shall determine if there is cause for such member to be restricted from reviewing, discussing, or possessing such information.

"(B) ACCESS.—

"(i) PROTECTED INFORMATION.—If the Director does not restrict a member from reviewing, discussing, or possessing sensitive information under subparagraph

(A) and the member voluntarily signs a nondisclosure agreement with respect to protected information, the member may be granted access to protected information that the Director determines is relevant to such member's service on the Advisory Committee.

"(ii) CLASSIFIED INFORMATION.—Access to classified materials shall be managed in accordance with Executive Order No. 13526 of December 29, 2009 (75 Fed. Reg 707), or any subsequent corresponding Executive Order.

"(C) PROTECTIONS.—A member of the Advisory Committee shall agree, as a condition of such membership, to protect all classified information in accordance with the applicable requirements for the particular level of classification of such information and to protect all protected information appropriately.

"(D) PROTECTED INFORMATION DEFINED.—In this section, the term 'protected information' means—

"(i) information specifically exempted from disclosure by statute or regulation;

1 ''(ii) trade secrets and commercial or
2 financial information obtained from a per-
3 son and privileged or confidential;
4 ''(iii) deliberative process privileged
5 information;
6 ''(iv) personally identifiable informa-
7 tion, the disclosure of which would con-
8 stitute an invasion of personal privacy;
9 ''(v) records containing law enforce-
10 ment sensitive information; and
11 ''(vi) other categories of information,
12 as determined by the Director.
13 ''(7) CHAIRPERSON.—The Advisory Committee
14 shall select, from among the members of the Advi-
15 sory Committee—
16 ''(A) a member to serve as chairperson of
17 the Advisory Committee; and
18 ''(B) a member to serve as chairperson of
19 each subcommittee of the Advisory Committee
20 established under subsection (d).
21 ''(d) SUBCOMMITTEES.—
22 ''(1) IN GENERAL.—The Director and the Advi-
23 sory Committee shall establish subcommittees within
24 the Advisory Committee to address cybersecurity
25 issues, including relating to the following:

1 ''(A) Information exchange.
2 ''(B) Critical infrastructure.
3 ''(C) Risk management.
4 ''(D) Public and private partnerships.
5 ''(2) ADDITIONAL SUBCOMMITTEES.—In addi-
6 tion to the subcommittees established pursuant to
7 paragraph (1), the Advisory Committee chairperson,
8 in coordination with the Director, may establish
9 within the Advisory Committee additional sub-
10 committees that the Director and Advisory Com-
11 mittee determine to be necessary.
12 ''(3) MEETINGS AND REPORTING.—Each sub-
13 committee shall meet at least bimonthly, and submit
14 to the Advisory Committee for inclusion in the an-
15 nual report required under subsection (b)(4) infor-
16 mation, including activities, findings, and rec-
17 ommendations, regarding subject matter considered
18 by the subcommittee.
19 ''(4) SUBJECT MATTER EXPERTS.—The chair of
20 the Advisory Committee shall appoint members to
21 subcommittees and shall ensure that each member
22 appointed to a subcommittee has subject matter ex-
23 pertise relevant to the subject matter of the sub-
24 committee.

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

(b) CLERICAL AMENDMENT.—The table of contents in section 1(b) of such Act is amended by inserting after the item relating to section 2214 the following new item:

"Sec. 2215. Cybersecurity Advisory Committee.".

SEC. 302. CYBERSECURITY ESSENTIALS.

(a) IN GENERAL.—Subsection (b) of section 2203 of the Homeland Security act of 2002 (6 U.S.C. 653) is amended—

(1) in paragraph (3), by striking "and" after the semicolon at the end;

(2) by redesignating paragraph (4) as paragraph (5); and

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

"(4) develop, publish and update as necessary guidelines and processes for a national audience regarding best practices for effective and usable basic controls that have the most impact in defending again common cybersecurity threats and cybersecurity risks; and".

(b) RESTRICTION.—Chapter 35 of title 44, United States Code (commonly known as the "Paperwork Reduc-

tion Act'') shall not apply to any action to implement this Act.

SEC. 303. ESTABLISHMENT OF CONTINUOUS DIAGNOSTICS AND MITIGATION PROGRAM IN THE CYBERSECURITY AND INFRASTRUCTURE SECURITY AGENCY.

(a) IN GENERAL.—Section 2213 of the Homeland Security Act of 2002 (6 U.S.C. 663) is amended by adding at the end the following new subsection:

''(g) CONTINUOUS DIAGNOSTICS AND MITIGATION.—

''(1) PROGRAM.—

''(A) IN GENERAL.—The Secretary, acting through the Director of Cybersecurity and Infrastructure Security, shall deploy, operate, and maintain a continuous diagnostics and mitigation program for agencies. Under such program, the Secretary shall—

''(i) assist agencies to continuously diagnose and mitigate cyber threats and vulnerabilities;

''(ii) develop and provide the capability to collect, analyze, and visualize information relating to security data and cybersecurity risks at agencies;

1 ''(iii) make program capabilities avail-
2 able for use, with or without reimburse-
3 ment, to civilian agencies and State, local,
4 Tribal, and territorial governments;
5 ''(iv) employ shared services, collective
6 purchasing, blanket purchase agreements,
7 and any other economic or procurement
8 models the Secretary determines appro-
9 priate to maximize the costs savings asso-
10 ciated with implementing an information
11 system;
12 ''(v) develop policies and procedures
13 for reporting systemic cybersecurity risks
14 and potential incidents based upon data
15 collected under such program.
16 ''(B) REGULAR IMPROVEMENT.—The Sec-
17 retary shall regularly deploy new technologies
18 and modify existing technologies to the contin-
19 uous diagnostics and mitigation program re-
20 quired under subparagraph (A), as appropriate,
21 to improve the program.
22 ''(2) AGENCY RESPONSIBILITIES.—Notwith-
23 standing any other provision of law, each agency
24 that uses the continuous diagnostics and mitigation
25 program under paragraph (1) shall, continuously

and in real time, provide to the Secretary all information, assessments, analyses, and raw data collected by the program, in a manner specified by the Secretary.

"(3) RESPONSIBILITIES OF THE SECRETARY.—In carrying out the continuous diagnostics and mitigation program under paragraph (1), the Secretary shall, as appropriate—

"(A) share with agencies relevant analysis and products developed under such program;

"(B) provide regular reports on cybersecurity risks to agencies; and

"(C) provide comparative assessments of cybersecurity risks for agencies.".

(b) CONTINUOUS DIAGNOSTICS AND MITIGATION STRATEGY.—

(1) IN GENERAL.—Not later than 180 days after the date of the enactment of this Act, the Secretary of Homeland Security shall develop a comprehensive continuous diagnostics and mitigation strategy to carry out the continuous diagnostics and mitigation program required under subsection (g) of section 2213 of the Homeland Security Act of 2002 (6 U.S.C. 663), as added by subsection (a).

(2) SCOPE.—The strategy required under paragraph (1) shall include the following:

(A) A description of the continuous diagnostics and mitigation program, including efforts by the Secretary of Homeland Security to assist with the deployment of program tools, capabilities, and services, from the inception of the program referred to in paragraph (1) to the date of enactment of this Act.

(B) A description of the coordination and funding required to deploy, install, and maintain the tools, capabilities, and services that the Secretary of Homeland Security determines to be necessary to satisfy the requirements of such program.

(C) A description of any obstacles facing the deployment, installation, and maintenance of tools, capabilities, and services under such program.

(D) Recommendations and guidelines to help maintain and continuously upgrade tools, capabilities, and services provided under such program.

(E) Recommendations for using the data collected by such program for creating a com-

1 mon framework for data analytics, visualization
2 of enterprise-wide risks, and real-time report-
3 ing, and comparative assessments for cyberse-
4 curity risks.
5 (F) Recommendations for future efforts
6 and activities, including for the rollout of new
7 and emerging tools, capabilities and services,
8 proposed timelines for delivery, and whether to
9 continue the use of phased rollout plans, related
10 to securing networks, devices, data, and infor-
11 mation and operational technology assets
12 through the use of such program.
13 (3) FORM.—The strategy required under para-
14 graph (1) shall be submitted in an unclassified form,
15 but may contain a classified annex.
16 (c) REPORT.—Not later than 180 days after the de-
17 velopment of the strategy required under subsection (b),
18 the Secretary of Homeland Security shall submit to the
19 Committee on Homeland Security and Governmental Af-
20 fairs of the Senate and the Committee on Homeland Secu-
21 rity of the House of Representative a report on cybersecu-
22 rity risk posture based on the data collected through the
23 continuous diagnostics and mitigation program under sub-
24 section (g) of section 2213 of the Homeland Security Act
25 of 2002 (6 U.S.C. 663), as added by subsection (a).

(d) GAO REPORT.—Not later than 1 year after the date of enactment of this Act, the Comptroller General of the United States shall submit a report to Congress on the potential impacts and benefits of replacing the reporting requirements under chapter 35 of title 44, United States Code, with periodical real-time data provided by the continuous diagnostics and mitigation program under subsection (g) of section 2213 of the Homeland Security Act of 2002 (6 U.S.C. 663), as added by subsection (a).

SEC. 304. ADMINISTRATIVE SUBPOENA AUTHORITY.

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

(1) in subsection (a)—

(A) by redesignating paragraph (6) as paragraph (7); and

(B) by inserting after paragraph (5) the following:

''(6) the term 'security vulnerability' has the meaning given that term in section 102(17) of the Cybersecurity Information Sharing Act of 2015 (615 U.S.C. 1501(17));'';

(2) in subsection (c)—

(A) in paragraph (10), by striking ''and'' at the end;

(B) in paragraph (11), by striking the period at the end and inserting "; and"; and

(C) by adding at the end the following:

"(12) detecting, identifying, and receiving information about security vulnerabilities relating to critical infrastructure in the information systems and devices of Federal and non-Federal entities for a cybersecurity purpose, as defined in section 102 of the Cybersecurity Information Sharing Act of 2015 (6 U.S.C. 1501), and notifying the owners and operators of critical infrastructure with such security vulnerability."; and

(3) by adding at the end the following:

"(n) SUBPOENA AUTHORITY.—

"(1) DEFINITION.—In this subsection, the term 'enterprise device or system'—

"(A) means a device or system commonly used to perform industrial, commercial, scientific, or governmental functions or processes that relate to critical infrastructure, including operational and industrial control systems, distributed control systems, and programmable logic controllers; and

"(B) does not include personal devices and systems, such as consumer mobile devices, home

1 computers, residential wireless routers, or resi-
2 dential Internet enabled consumer devices.
3 ''(2) AUTHORITY.—
4 ''(A) IN GENERAL.—If the Director identi-
5 fies a system connected to the internet which he
6 reasonably believes contains a with a specific se-
7 curity vulnerability and reasonably believes that
8 the security vulnerability relates to critical in-
9 frastructure and affects an enterprise device or
10 system owned or operated by a Federal or non-
11 Federal entity, and the Director is unable to
12 identify the entity at risk, the Director may
13 issue a subpoena for the production of informa-
14 tion necessary to identify and notify the entity
15 at risk, in order to carry out a function author-
16 ized under subsection (c)(12).
17 ''(B) LIMIT ON INFORMATION.—A sub-
18 poena issued under the authority under sub-
19 paragraph (A) may only seek information in the
20 categories set forth in subparagraphs (A), (B),
21 (D), and (E) of section 2703(c)(2) of title 18,
22 United States Code.
23 ''(C) LIABILITY PROTECTIONS FOR DIS-
24 CLOSING PROVIDERS.—The provisions of section
25 2703(e) of title 18, United States Code, shall

apply to any subpoena issued under the authority under subparagraph (A).

"(3) COORDINATION.—

"(A) IN GENERAL.—If the Director decides to exercise the subpoena authority under this subsection, and in the interest of avoiding interference with ongoing law enforcement investigations, the Director shall coordinate the issuance of any such subpoena with the Department of Justice, including the Federal Bureau of Investigation, pursuant to inter-agency procedures which the Director, in coordination with the Attorney General, shall develop not later than 60 days after the date of enactment of this subsection.

"(B) CONTENTS.—The inter-agency procedures developed under this paragraph shall provide that a subpoena issued by the Director under this subsection shall be—

"(i) issued in order to carry out a function described in subsection (c)(12); and

"(ii) subject to the limitations under this subsection.

1 "(C) RESTRICTION ON LAW ENFORCEMENT
2 USE.—The regulations or guidance issued to
3 carry out actions authorized under subsection
4 (n) by the Director may not be used by the De-
5 partment of Justice, including the Federal Bu-
6 reau of Investigation, to predicate a new inves-
7 tigation solely on the information contained in
8 a subpoena issued under subsection (n).
9 "(4) NONCOMPLIANCE.—If any person, part-
10 nership, corporation, association, or entity fails to
11 comply with any duly served subpoena issued under
12 this subsection, the Director may request that the
13 Attorney General seek enforcement of the subpoena
14 in any judicial district in which such person, part-
15 nership, corporation, association, or entity resides, is
16 found, or transacts business.
17 "(5) NOTICE.—Not later than 7 days after the
18 date on which the Director receives information ob-
19 tained through a subpoena issued under this sub-
20 section, the Director shall notify the entity at risk
21 identified by information obtained under the sub-
22 poena regarding the subpoena and the identified vul-
23 nerability.
24 "(6) AUTHENTICATION.—Any subpoena issued
25 by the Director under this subsection shall be au-

1 thenticated by the electronic signature of an author-
2 ized representative of the Agency or other com-
3 parable symbol or process identifying the Agency as
4 the source of the subpoena.

5 "(7) REMEDIATION.—Upon successful identi-
6 fication of a vulnerability on a system owned or op-
7 erated by the party or entity, the Director shall,
8 upon request—

9 "(A) provide appropriate, detailed technical
10 guidance to remediate, end, or mitigate the vul-
11 nerability identified by the subpoena;

12 "(B) provide appropriate, detailed tech-
13 nical guidance to prevent a recurrence or the
14 vulnerability or a similar vulnerability in the fu-
15 ture; and

16 "(C) provide appropriate information re-
17 garding any other exploitable vulnerabilities dis-
18 covered on a system owned or operated by a
19 party or entity during the course of investiga-
20 tion and remediation operations by the Agency.

21 "(8) PROCEDURES.—Not later than 90 days
22 after the date of enactment of this subsection, the
23 Director shall establish internal procedures and as-
24 sociated training, applicable to employees and oper-

1 ations of the Agency, regarding subpoenas issued
2 under this subsection, which shall address—
3 ''(A) the protection of and restriction on
4 dissemination of nonpublic information obtained
5 through a subpoena issued under this sub-
6 section, including a requirement that the Agen-
7 cy shall not disseminate nonpublic information
8 obtained through a subpoena issued under this
9 subsection that identifies the party that is sub-
10 ject to the subpoena or the entity at risk identi-
11 fied by information obtained, unless—
12 ''(i) the party or entity consents; or
13 ''(ii) the Agency identifies or is noti-
14 fied of a cybersecurity incident involving
15 the party or entity, which relates to the
16 vulnerability which led to the issuance of
17 the subpoena;
18 ''(B) the restriction on the use of informa-
19 tion obtained through the subpoena for a cyber-
20 security purpose, as defined in section 102 of
21 the Cybersecurity Information Sharing Act of
22 2015 (6 U.S.C. 1501);
23 ''(C) the retention and destruction of non-
24 public information obtained through a subpoena
25 issued under this subsection, including—

1 ''(i) immediate destruction of informa-
2 tion obtained through the subpoena that
3 the Director determines is unrelated to
4 critical infrastructure; and
5 ''(ii) destruction of any personally
6 identifiable information not later than 6
7 months after the date on which the Direc-
8 tor receives information obtained through
9 the subpoena, unless otherwise agreed to
10 by the individual identified by the sub-
11 poena respondent;
12 ''(D) the processes for providing notice to
13 each party that is subject to the subpoena and
14 each entity at risk identified by information ob-
15 tained pursuant to a subpoena issued under
16 this subsection;
17 ''(E) the processes and criteria for con-
18 ducting critical infrastructure security risk as-
19 sessments to determine whether a subpoena is
20 necessary prior to being issued under this sub-
21 section; and
22 ''(F) the processes for assisting a party or
23 entity with removal, remediation, or other cor-
24 rective measures required to address the vulner-
25 ability identified by the subpoena and, upon re-

quest, providing other resources to parties or entities to prevent a recurrence of the vulnerability or a related vulnerability in the future.

''(9) REVIEW OF PROCEDURES.—Not later than 1 year after the date of enactment of this subsection, the Privacy Officer of the Agency shall—

''(A) review the procedures developed by the Director under paragraph (8) to ensure that—

''(i) the procedures are consistent with fair information practices; and

''(ii) the operations of the Agency comply with the procedures; and

''(B) notify the Committee on Homeland Security and Governmental Affairs of the Senate and the Committee on Homeland Security of the House of Representatives of the results of the review.

''(10) PUBLICATION OF INFORMATION.—Not later than 120 days after establishing the internal procedures under paragraph (8), the Director shall make publicly available information regarding the subpoena process under this subsection, including regarding—

"(A) the purpose for subpoenas issued under this subsection;

"(B) the subpoena process;

"(C) the criteria for the critical infrastructure security risk assessment conducted prior to issuing a subpoena;

"(D) policies and procedures on retention and sharing of data obtained by subpoena;

"(E) guidelines on how entities contacted by the Director may respond to notice of a subpoena; and

"(F) the procedures and policies of the Agency developed under paragraph (8).

"(11) ANNUAL REPORTS.—The Director shall annually submit to the Committee on Homeland Security and Governmental Affairs of the Senate and the Committee on Homeland Security of the House of Representatives a report (which may include a classified annex but with the presumption of declassification) on the use of subpoenas under this subsection by the Director, which shall include—

"(A) a discussion of—

"(i) the effectiveness of the use of subpoenas to mitigate critical infrastructure security vulnerabilities;

1 ''(ii) the critical infrastructure secu-
2 rity risk assessment process conducted for
3 subpoenas issued under this subsection;
4 ''(iii) the number of subpoenas issued
5 under this subsection by the Director dur-
6 ing the preceding year;
7 ''(iv) to the extent practicable, the
8 number of vulnerable enterprise devices or
9 systems mitigated under this subsection by
10 the Agency during the preceding year; and
11 ''(v) the number of entities notified by
12 the Director under this subsection, and
13 their response, during the previous year;
14 and
15 ''(B) for each subpoena issued under this
16 subsection—
17 ''(i) the source of the security vulner-
18 ability detected, identified, or received by
19 the Director;
20 ''(ii) the steps taken to identify the
21 entity at risk prior to issuing the sub-
22 poena; and
23 ''(iii) a description of the outcome of
24 the subpoena, including discussion on the

resolution or mitigation of the critical infrastructure security vulnerability.

"(12) PUBLICATION OF THE ANNUAL REPORTS.—The Director shall make a version of the annual report required by paragraph (11) publicly available, which shall, at a minimum, include the findings described in clause (iii), (iv) and (v) of subparagraph (A).".

SEC. 305. CISA DIRECTOR TERM LIMITATION.

(a) IN GENERAL.—Subsection (b) of section 2202 of the Homeland Security Act of 2002 (6 U.S.C. 652) is amended by—

(1) redesignating paragraph (2) as paragraph (3); and

(2) inserting after paragraph (1) the following new paragraph:

"(2) TERM.—Effective with respect to an individual appointed to be the Director by the President, by and with the advice and consent of the Senate, after the date of the enactment of this paragraph, the term of office of such an individual so appointed shall be five years, and such an individual may not serve more than two terms. The term of office of the individual serving as the Director as of such date of

enactment shall be five years beginning on the date on which the Director began serving.''.

(b) AMENDMENT RELATING TO QUALIFICATIONS FOR CERTAIN CISA ASSISTANT DIRECTORS.—The Homeland Security Act of 2002 is amended—

(1) in subparagraph (B) of section 2203(a)(2) (6 U.S.C. 653(a)(2)), by striking ''President without the advice and consent of the Senate'' and inserting ''Secretary''; and

(2) in subparagraph (B) of section 2204(a)(2) (6 U.S.C. 654(a)(2)), by striking ''President without the advice and consent of the Senate'' and inserting ''Secretary''.

(c) AMENDMENT TO POSITION LEVEL OF CISA DIRECTOR.—Subchapter II of chapter 53 of title 5, United States Code, is amended—

(1) in section 5313, by inserting after ''Administrator of the Transportation Security Administration.'' the following:

''Director, Cybersecurity and Infrastructure Security Agency.''; and

(2) in section 5314, by striking ''Director, Cybersecurity and Infrastructure Security Agency.''.

SEC. 306. STATE, LOCAL, TRIBAL AND TERRORITORIAL CYBERSECURITY.

(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 this title, is further amended by adding at the end the following new sections:

"SEC. 2216. CYBERSECURITY RESOURCE GUIDE DEVELOPMENT FOR STATE, AND LOCAL, TRIBAL, AND TERRITORIAL GOVERNMENT OFFICIALS.

"The Secretary, acting through the Director, shall develop a resource guide for use by State, local, and Tribal officials, including law enforcement officers, to help such officials prepare for, protect against, respond to, recover from, and mitigate against cyber attacks.

"SEC. 2217. STATE, LOCAL, TRIBAL, AND TERRITORIAL CYBERSECURITY GRANTS.

"(a) IN GENERAL.—The Director shall establish a State, local, Tribal, and territorial government cybersecurity initiative to make grants to State, local, Tribal, and territorial governments to prepare for, protect against, respond to, recover from, and mitigate against cyber attacks.

"(b) APPLICATION.—

"(1) IN GENERAL.—Each State, local, Tribal, and territorial government may apply for a grant under this section, and shall submit such informa-

tion in support of an application relating thereto as the Director may require.

"(2) MINIMUM CONTENTS OF APPLICATION.—An application under this subsection shall include the following:

"(A) A description of how the State, local, Tribal, or territorial government plans to allocate grant funds.

"(B) A budget showing how the State, local, Tribal, or territorial government intends to expend grant funds.

"(3) DURATION.—Grants under this section shall be for one year, and a State, local, Tribal, or territorial government may apply or reapply on an annual basis.

"(c) GRANT AWARD.—To be eligible to receive a grant under this section, a State, local, Tribal, or territorial government shall agree to contribute, from State or local government appropriated funds, other State or local government revenue, or from private contributions received by the State or local government, not less than 20 percent of the amount of the grant.

"(d) AUTHORIZATION OF APPROPRIATIONS.—There is authorized to be appropriated $50,000,000 for each of fiscal years 2020 through 2024 and such sums as may

be necessary for each fiscal year thereafter to carry out 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 2215, as added by this title, the following new items:

''Sec. 2216. Cybersecurity resource guide development for State and local government officials.
''Sec. 2217. State, local, Tribal, and territorial cybersecurity grants.''.

(c) ADDITIONAL REQUIREMENTS.—Subtitle A of title XXII of the Homeland Security Act of 2002 (6 U.S.C 652 et seq.), as amended by this title, is further amended—

(1) in section 2201 (6 U.S.C. 651)—

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

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

''(4) ENTITY.—The term 'entity' shall include—

''(A) an association, corporation, whether for-profit or nonprofit, partnership, proprietorship, organization, institution, establishment, or individual, whether domestic or foreign;

''(B) a government agency or other governmental entity, whether domestic or foreign, in-

1 cluding State, local, Tribal, and territorial gov-
2 ernment entities; and
3 ''(A) the general public.''; ad
4 (2) in section 2209 (6 U.S.C. 659), by adding
5 at the end the following new subsection:
6 ''(n) COORDINATION.—The Director shall, to the ex-
7 tent practicable, and in coordination as appropriate with
8 Federal and non-Federal entities, such as the Multi-State
9 Information Sharing and Analysis Center—
10 ''(1) conduct exercises with Federal and non-
11 Federal entities;
12 ''(2) provide operational and technical cybersec-
13 urity training related to cyber threat indicators, de-
14 fensive measures, cybersecurity risks, and incidents
15 to Federal and non-Federal entities to address cy-
16 bersecurity risks or incidents, with or without reim-
17 bursement;
18 ''(3) assist Federal and non-Federal entities,
19 upon request, in sharing cyber threat indicators, de-
20 fensive measures, cybersecurity risks, and incidents
21 from and to the Federal Government as well as
22 among Federal and non-Federal entities, in order to
23 increase situational awareness and help prevent inci-
24 dents;

1 ''(4) provide Federal and non-Federal entities
2 timely notifications containing specific incident and
3 malware information that may affect such entities or
4 individuals with respect to whom such entities have
5 a relationship;
6 ''(5) provide and periodically update via a web
7 portal and other means tools, products, resources,
8 policies, guidelines, controls, procedures and other
9 cybersecurity standards and best practices and pro-
10 cedures related to information security;
11 ''(6) work with senior Federal and non-Federal
12 officials, including State and local Chief Information
13 Officers, senior election officials, and through na-
14 tional associations, to coordinate a nationwide effort
15 to ensure effective implementation of tools, products,
16 resources, policies, guidelines, controls, procedures,
17 and other cybersecurity standards and best practices
18 and procedures related to information security to se-
19 cure and ensure the resiliency of Federal and non-
20 Federal information systems and including election
21 systems;
22 ''(7) provide, upon request, operational and
23 technical assistance to Federal and non-Federal enti-
24 ties to implement tools, products, resources, policies,
25 guidelines, controls, procedures, and other cyberse-

curity standards and best practices related to information security, including by, as appropriate, deploying and sustaining cybersecurity technologies, such as an intrusion detection capability, to assist such Federal and non-Federal entities in detecting cybersecurity risks and incidents;

''(8) assist Federal and non-Federal entities in developing policies and procedures for coordinating vulnerability disclosures, to the extent practicable, consistent with international and national standards in the information technology industry;

''(9) ensure that Federal and non-Federal entities, as appropriate, are made aware of the tools, products, resources, policies, guidelines, controls, procedures, and other cybersecurity standards and best practices related to information security developed by the Department and other appropriate Federal entities for ensuring the security and resiliency of civilian information systems; and

''(10) promote cybersecurity education and awareness through engagements with Federal and non-Federal entities.''.

SEC. 307. CYBERSECURITY WORKFORCE.

(a) CYBERSECURITY TALENT EXCHANGE.—

(1) DEFINITIONS.—In this section—

(A) the term ''congressional homeland security committees'' means—

(i) the Committee on Homeland Security and Governmental Affairs and the Committee on Appropriations of the Senate; and

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

(B) the term ''Department'' means the Department of Homeland Security; and

(C) the term ''Secretary'' means the Secretary of Homeland Security.

(2) CYBERSECURITY TALENT EXCHANGE PILOT PROGRAM.—

(A) IN GENERAL.—Not later than 1 year after the date of enactment of this Act, the Secretary shall commence carrying out a cybersecurity talent exchange pilot program.

(B) DELEGATION.—The Secretary may delegate any authority under this section to the Director of the Cybersecurity and Infrastructure Security Agency of the Department.

(3) APPOINTMENT AUTHORITY.—

(A) IN GENERAL.—Under regulations prescribed by the Secretary for the purpose of carrying out the pilot program established under subsection (b), the Secretary may, with the agreement of a private-sector organization and the consent of the employee, arrange for the temporary assignment of an employee to the private-sector organization, or from the private-sector organization to a Department organization under this section.

(B) ELIGIBLE EMPLOYEES.—Employees participating in the pilot program established under subsection (b) shall have significant education, skills, or experience relating to cybersecurity.

(C) AGREEMENTS.—

(i) IN GENERAL.—The Secretary shall provide for a written agreement among the Department, the private-sector organization, and the employee concerned regarding the terms and conditions of the assignment of the employee under this section, which—

(I) shall require that the employee of the Department, upon com-

1 pletion of the assignment, will serve in
2 the Department, or elsewhere in the
3 civil service if approved by the Sec-
4 retary, for a period equal to twice the
5 length of the assignment;
6 (II) shall provide that if the em-
7 ployee of the Department or of the
8 private-sector organization, as the
9 case may be, fails to carry out the
10 agreement, the employee shall be lia-
11 ble to the United States for payment
12 of all expenses of the assignment, un-
13 less that failure was for good and suf-
14 ficient reason, as determined by the
15 Secretary;
16 (III) shall contain language en-
17 suring that the employee of the De-
18 partment does not improperly use pre-
19 decisional or draft deliberative infor-
20 mation that the employee may be
21 privy to or aware of related to De-
22 partment programing, budgeting,
23 resourcing, acquisition, or procure-
24 ment for the benefit or advantage of
25 the private-sector organization; and

(IV) shall cover matters relating to confidentiality, intellectual property rights, and such other matters as the Secretary considers appropriate.

(ii) LIABILITY.—An amount for which an employee is liable under subparagraph (i)(II) shall be treated as a debt due the United States.

(iii) WAIVER.—The Secretary may waive, in whole or in part, collection of a debt described in subparagraph (B) based on a determination that the collection would be against equity and good conscience and not in the best interests of the United States, after taking into account any indication of fraud, misrepresentation, fault, or lack of good faith on the part of the employee.

(D) TERMINATION.—An assignment under this subsection may, at any time and for any reason, be terminated by the Department or the private-sector organization concerned.

(E) DURATION.—

(i) IN GENERAL.—Except as provided in subparagraph (B), an assignment under

this subsection shall be for a period of not less than 3 months and not more than 2 years, and renewable up to a total of 4 years.

(ii) EXCEPTION.—An assignment under this subsection may be for a period in excess of 2 years, but not more than 4 years, if the Secretary determines that the assignment is necessary to meet critical mission or program requirements.

(iii) LIMITATION.—No employee of the Department may be assigned under this subsection for more than a total of 4 years inclusive of all assignments.

(F) STATUS OF FEDERAL EMPLOYEES ASSIGNED TO PRIVATE-SECTOR ORGANIZATIONS.—

(i) IN GENERAL.—An employee of the Department who is assigned to a private-sector organization under this subsection shall be considered, during the period of assignment, to be on detail to a regular work assignment in the Department for all purposes.

(ii) WRITTEN AGREEMENT.—The written agreement established under para-

graph (3) shall address the specific terms and conditions related to the continued status of the employee as a Federal employee.

(iii) CERTIFICATION.—In establishing a temporary assignment of an employee of the Department to a private-sector organization, the Secretary shall—

(I) ensure that the normal duties and functions of the employee can be reasonably performed by other employees of the Department without the transfer or reassignment of other personnel of the Department; and

(II) certify that the temporary assignment of the employee shall not have an adverse or negative impact on organizational capabilities associated with the assignment.

(G) TERMS AND CONDITIONS FOR PRIVATE-SECTOR EMPLOYEES.—An employee of a private-sector organization who is assigned to a Department organization under this subsection—

(i) shall continue to receive pay and benefits from the private-sector organization from which the employee is assigned and shall not receive pay or benefits from the Department, except as provided in subparagraph (B);

(ii) is deemed to be an employee of the Department for the purposes of—

(I) chapters 73 and 81 of title 5, United States Code;

(II) sections 201, 203, 205, 207, 208, 209, 603, 606, 607, 643, 654, 1905, and 1913 of title 18, United States Code;

(III) sections 1343, 1344, and 1349(b) of title 31, United States Code;

(IV) chapter 171 of title 28, United States Code (commonly known as the ''Federal Tort Claims Act'') and any other Federal tort liability statute;

(V) the Ethics in Government Act of 1978 (5 U.S.C. App.); and

(VI) chapter 21 of title 41, United States Code;

(iii) shall not have access to any trade secrets or to any other nonpublic information which is of commercial value to the private-sector organization from which the employee is assigned;

(iv) may perform work that is considered inherently governmental in nature only when requested in writing by the Secretary; and

(v) may not be used to circumvent any limitation or restriction on the size of the workforce of the Department.

(H) PROHIBITION AGAINST CHARGING CERTAIN COSTS TO THE FEDERAL GOVERNMENT.—A private-sector organization may not charge the Department or any other agency of the Federal Government, as direct or indirect costs under a Federal contract, the costs of pay or benefits paid by the organization to an employee assigned to a Department organization under this subsection for the period of the assignment.

(I) EXPENSES.—

(i) IN GENERAL.—The Secretary may pay for travel and other work-related expenses associated with individuals participating in the pilot program established under subsection (b). The Secretary shall not pay for lodging or per diem expenses for employees of a private sector organization, unless such expenses are in furtherance of work-related travel other than participating in the pilot program.

(ii) BACKGROUND INVESTIGATION.—A private person supporting an individual participating in the pilot program may pay for a background investigation associated with the participation of the individual in the pilot program.

(J) MAXIMUM NUMBER OF PARTICIPANTS.—Not more than 250 individuals may concurrently participate in the pilot program established under subsection (b).

(4) DETAILING OF PARTICIPANTS.—With the consent of an individual participating in the pilot program established under subsection (b), the Secretary may, under the pilot program, detail the individual to another Federal department or agency.

(5) SUNSET.—The pilot program established under subsection (b) shall terminate on the date that is 7 years after the date of enactment of this Act.

(6) REPORTS.—

(A) PRELIMINARY REPORT.—Not later than 2 years after the date of enactment of this Act, the Secretary shall submit to the congressional homeland security committees a preliminary report describing the implementation of the pilot program established under subsection (b), including the number of participating employees from the Department and from private sector organizations, the departmental missions or programs carried out by employees participating in the pilot program, and recommendations to maximize efficiencies and the effectiveness of the pilot program in order to support Department cybersecurity missions and objectives.

(B) FINAL REPORT.—Not later than 6 years after the date of enactment of this Act, the Secretary shall submit to the congressional homeland security committees a final report describing the implementation of the pilot program established under subsection (b), includ-

ing the number of participating employees from the Department and from private sector organizations, the departmental missions or programs carried out by employees participating in the pilot program, and providing a recommendation on whether the pilot program should be made permanent.

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

"SEC. 2218. CYBERSECURITY APPRENTICESHIPS.

''The director of cybersecurity and infrastructure security agency may establish a cybersecurity apprenticeship program in coordination with the National Institutes of Standards and Technology National Initiative for Cybersecurity Education and the Department of Labor Apprenticeship Office.''.

(c) 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 2217, as added by this title, the following new item:

''Sec. 2218. Cybersecurity apprenticeships.''.

SEC. 308. ELECTION SECURITY.

(a) ELECTION INFRASTRUCTURE DESIGNATION.—Subparagraph (J) of section 2001(3) of the Homeland Se-

1 curity Act of 2002 (6 U.S.C. 601(3)) is amended by in-
2 serting ", including election infrastructure" before the pe-
3 riod at the end.

4 (b) TIMELY THREAT INFORMATION.—Subsection (d)
5 of section 201 of the Homeland Security Act of 2002 (6
6 U.S.C. 121), as amended by title II of this Act, is further
7 amended by adding at the end the following new para-
8 graph:

9 "(25) To provide timely threat information re-
10 garding election infrastructure to the chief State
11 election official of the State with respect to which
12 such information pertains.".

13 (c) ELECTION SECURITY RESPONSIBILITIES.—In
14 carrying out the responsibilities under section 2202 of the
15 Homeland Security Act of 2002 (6 U.S.C. 652), the Direc-
16 tor of Cybersecurity and Infrastructure Security Agency
17 may—

18 (1) upon request, provide State and local elec-
19 tion jurisdictions, with—

20 (A) technical assistance with election infra-
21 structure;

22 (B) cyber hygiene service for internet-fac-
23 ing systems;

24 (C) risk and vulnerability assessments;

25 (D) incident response assistance; and

(E) provide physical and protective security tools, training and resources; and

(2) employ field-base cybersecurity advisors and protective security advisors.

SEC. 309. PROTECTION FROM LIABILITY.

Section 2224 of the Homeland Security Act (6 U.S.C. 673) is amending by adding at the end the following new subsections:

''(i) MONITORING OF INFORMATION SYSTEMS.—No cause of action shall lie or be maintained in any court against any private entity, and such action shall be promptly dismissed, for the monitoring of an information system and information under section 104(a) that is conducted in accordance with this title.

''(j) SHARING OR RECEIPT OF CYBER THREAT INDICATORS.—

''(1) IN GENERAL.—No cause of action shall lie or be maintained in any court against any private entity, and such action shall be promptly dismissed, for the sharing or receipt of a cyber threat indicator or defensive measure under section 104(c) if—

''(A) such sharing or receipt is conducted in accordance with this title; and

''(B) in a case in which a cyber threat indicator or defensive measure is shared with the

Federal Government, the cyber threat indicator or defensive measure is shared in a manner that is consistent with section 105(c)(1)(B) and the sharing or receipt, as the case may be, occurs after the earlier of—

"(i) the date on which the interim policies and procedures are submitted to Congress under section 105(a)(1) and guidelines are submitted to Congress under section 105(b)(1); or

"(ii) the date that is 60 days after the date of the enactment of this subsection.

"(2) RULE OF CONSTRUCTION.—Nothing in this subsection may be construed to—

"(A) create a duty to—

"(i) share a cyber threat indicator or defensive measure; or

"(ii) warn or act based on the receipt of a cyber threat indicator or defensive measure; or

"(B) undermine or limit the availability of otherwise applicable common law or statutory defenses.".

SEC. 310. PERMANENT EXTENSION OF CHEMICAL FACILITY ANTI-TERRORISM STANDARDS PROGRAM OF THE DEPARTMENT OF HOMELAND SECURITY.

Section 5 of the Protecting and Securing Chemical Facilities from Terrorist Attacks Act of 2014 (Public Law 113–254; 6 U.S.C. 621 note) is repealed.

SEC. 311. CYBERSECURITY RESEARCH AND DEVELOPMENT PROJECTS.

(a) CYBERSECURITY RESEARCH AND DEVELOPMENT.—

(1) IN GENERAL.—Title III of the Homeland Security Act of 2002 (6 U.S.C. 181 et seq.), as amended by title I of this Act, is further amended by adding at the end the following new section:

"SEC. 322. CYBERSECURITY RESEARCH AND DEVELOPMENT.

''(a) IN GENERAL.—The Under Secretary for Science and Technology shall support the research, development, testing, evaluation, and transition of cybersecurity technologies, including fundamental research to improve the sharing of information, information security, analytics, and methodologies related to cybersecurity risks and incidents, consistent with current law.

''(b) ACTIVITIES.—The research and development supported under subsection (a) shall serve the components of the Department and shall—

1 ''(1) advance the development and accelerate
2 the deployment of more secure information systems;
3 ''(2) improve and create technologies for detect-
4 ing and preventing attacks or intrusions, including
5 real-time continuous diagnostics, real-time analytic
6 technologies, and full life cycle information protec-
7 tion;
8 ''(3) improve and create mitigation and recov-
9 ery methodologies, including techniques and policies
10 for real-time containment of attacks and develop-
11 ment of resilient networks and information systems;
12 ''(4) assist the development and support infra-
13 structure and tools to support cybersecurity research
14 and development efforts, including modeling,
15 testbeds, and data sets for assessment of new cyber-
16 security technologies;
17 ''(5) assist the development and support of
18 technologies to reduce vulnerabilities in industrial
19 control systems;
20 ''(6) assist the development and support cyber
21 forensics and attack attribution capabilities;
22 ''(7) assist the development and accelerate the
23 deployment of full information life cycle security
24 technologies to enhance protection, control, and pri-

vacy of information to detect and prevent cybersecurity risks and incidents;

''(8) assist the development and accelerate the deployment of information security measures, in addition to perimeter-based protections;

''(9) assist the development and accelerate the deployment of technologies to detect improper information access by authorized users;

''(10) assist the development and accelerate the deployment of cryptographic technologies to protect information at rest, in transit, and in use;

''(11) assist the development and accelerate the deployment of methods to promote greater software assurance;

''(12) assist the development and accelerate the deployment of tools to securely and automatically update software and firmware in use, with limited or no necessary intervention by users and limited impact on concurrently operating systems and processes; and

''(13) assist in identifying and addressing unidentified or future cybersecurity threats.

''(c) COORDINATION.—In carrying out this section, the Under Secretary for Science and Technology shall coordinate activities with—

1 ''(1) the Director of Cybersecurity and Infra-
2 structure Security;
3 ''(2) the heads of other relevant Federal depart-
4 ments and agencies, as appropriate; and
5 ''(3) industry and academia.
6 ''(d) TRANSITION TO PRACTICE.—The Under Sec-
7 retary for Science and Technology shall—
8 ''(1) support projects carried out under this
9 title through the full life cycle of such projects, in-
10 cluding research, development, testing, evaluation,
11 pilots, and transitions;
12 ''(2) identify mature technologies that address
13 existing or imminent cybersecurity gaps in public or
14 private information systems and networks of infor-
15 mation systems, protect sensitive information within
16 and outside networks of information systems, iden-
17 tify and support necessary improvements identified
18 during pilot programs and testing and evaluation ac-
19 tivities, and introduce new cybersecurity technologies
20 throughout the homeland security enterprise through
21 partnerships and commercialization; and
22 ''(3) target federally funded cybersecurity re-
23 search that demonstrates a high probability of suc-
24 cessful transition to the commercial market within 2
25 years and that is expected to have a notable impact

on the public or private information systems and networks of information systems.

''(e) DEFINITIONS.—In this section:

''(1) CYBERSECURITY RISK.—The term 'cybersecurity risk' has the meaning given the term in section 2209.

''(2) HOMELAND SECURITY ENTERPRISE.—The term 'homeland security enterprise' means relevant governmental and nongovernmental entities involved in homeland security, including Federal, State, local, and Tribal government officials, private sector representatives, academics, and other policy experts.

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

''(4) INFORMATION SYSTEM.—The term 'information system' has the meaning given the term in section 3502 of title 44, United States Code.

''(5) SOFTWARE ASSURANCE.—The term 'software assurance' means confidence that software—

''(A) is free from vulnerabilities, either intentionally designed into the software or accidentally inserted at any time during the life cycle of the software; and

''(B) functioning in the intended manner.''.

(2) 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 321, as added by title I of this Act, the following new item:

"Sec. 322. Cybersecurity research and development.".

(b) RESEARCH AND DEVELOPMENT PROJECTS.—Section 831 of the Homeland Security Act of 2002 (6 U.S.C. 391) is amended—

(1) in subsection (a)—

(A) in the matter preceding paragraph (1), by striking "2017" and inserting "2022"; and

(B) in paragraph (2), by striking "under section 845 of the National Defense Authorization Act for Fiscal Year 1994 (Public Law 103–160). In applying the authorities of that section 845, subsection (c) of that section shall apply with respect to prototype projects under this paragraph, and the Secretary shall perform the functions of the Secretary of Defense under subsection (d) thereof" and inserting "under section 2371b of title 10, United States Code, and the Secretary shall perform the functions of the Secretary of Defense as prescribed.";

(2) in subsection (c)—

(A) in paragraph (1), in the matter preceding subparagraph (A), by striking ''2017'' and inserting ''2022''; and

(B) by amending paragraph (2) to read as follows:

''(2) REPORT.—The Secretary shall annually submit to the Committee on Homeland Security and the Committee on Science, Space, and Technology of the House of Representatives and the Committee on Homeland Security and Governmental Affairs of the Senate a report detailing the projects for which the authority granted by subsection (a) was utilized, the rationale for such utilizations, the funds spent utilizing such authority, the extent of cost-sharing for such projects among Federal and non-Federal sources, the extent to which utilization of such authority has addressed a homeland security capability gap or threat to the homeland identified by the Department, the total amount of payments, if any, that were received by the Federal Government as a result of the utilization of such authority during the period covered by each such report, the outcome of each project for which such authority was utilized, and the results of any audits of such projects.'';

(3) in subsection (d), by striking ''as defined in section 845(e) of the National Defense Authorization Act for Fiscal Year 1994 (Public Law 103–160; 10 U.S.C. 2371 note)'' and inserting ''as defined in section 2371b(e) of title 10, United States Code.''; and

(4) by adding at the end the following:

''(e) TRAINING.—The Secretary shall develop a training program for acquisitions staff on the utilization of the authority provided under subsection (a) to ensure accountability and effective management of projects consistent with the Program Management Improvement Accountability Act (Public Law 114–264; 130 Stat. 1371) and the amendments made by such Act.''.

(c) NO ADDITIONAL FUNDS AUTHORIZED.—No additional funds are authorized to carry out the requirements of this section and the amendments made by this section. Such requirements shall be carried out using amounts otherwise authorized.

SEC. 312. LOAN REPAYMENT PROGRAM.

(a) AGREEMENT.—The Secretary of Homeland Security shall enter into an agreement with each individual in a cybersecurity position identified by a Federal agency pursuant to section 303 of the Federal Cybersecurity Workforce Assessment Act of 2015, under which—

(1) the individual agrees serve in such a position for not less than a 5-year period; and

(2) for each year of such service, the Secretary shall repay an amount of principal and interest, as specified in the agreement, that the individual owes on qualifying educational loans.

(b) QUALIFYING EDUCATIONAL LOAN DEFINED.—The term ''qualifying educational loan'' means a loan made under part D of title IV of the Higher Education Act of 1965 (20 U.S.C. 1087a) or private education loan (as defined in section 140 of the Truth in Lending Act) received by an individual for the cost of attendance (as defined in section 472 of the Higher Education Act of 1965 (20 U.S.C. 1087ll) at an institution designated by the Department as a Center for Academic Excellence in Cybersecurity.

(c) BREACH REMEDIES.—

(1) IN GENERAL.—Subject to paragraph (1), an agreement under subsection (a) shall provide for remedies in a case in which an individual does not comply with the service requirement under subsection (a)(1), including repayment or partial repayment of the loan repayment amount received under subsection (a), with interest.

(2) WAIVER.—The Secretary of Homeland Security waive a remedy provided for under paragraph (1) in the case of extreme hardship or extreme need, as determined by the Secretary.

(d) ADMINISTRATION.—The Secretary of Homeland Security may carry out this section directly or enter into an agreement with another Federal agency or other service provider to assist in the administration of this section.

(e) REPAYMENT SCHEDULE.—The Secretary of Homeland Security may enter into an agreement with the holder of any loan for which the Secretary makes payments under this section to establish a schedule for the making of such payments.

(f) REGULATIONS.—Not later than 270 days after the date of enactment of this subsection, the Secretary of Homeland Security shall promulgate regulations to carry out this section, including regulations to determine the aggregate amount of loan repayment that an individual may receive under subsection (a).

SEC. 313. EXCLUSION OF CERTAIN STUDENT LOAN REPAYMENTS.

(a) IN GENERAL.—Part III of subchapter B of chapter 1 of the Internal Revenue Code of 1986 is amended by inserting after section 139H the following new section:

"SEC. 139I. CERTAIN STUDENT LOAN REPAYMENTS.

"Gross income shall not include any amount of loan repayment received under section 312(a) of the Keep America Secure Act.".

(b) CLERICAL AMENDMENT.—The table of sections for part III of subchapter B of chapter 1 of such Code is amended by inserting after the item relating to section 139H the following new item:

"Sec. 139I. Certain student loan repayments.".

(c) EFFECTIVE DATE.—The amendments made by this section shall apply to taxable years beginning after December 31, 2019.

SEC. 314. SCHOLARSHIP FOR SERVICE.

(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 this title, is further amended by adding at the end the following new section:

"SEC. 2219. SCHOLARSHIP FOR SERVICE.

"(a) IN GENERAL.—The Secretary, acting through the Director, may establish a scholarship program (in this section referred to as the 'program') to recruit and train information technology, cybersecurity, and industrial control system security professionals to work in the Agency.

"(b) ELEMENTS.—The program shall—

"(1) provide scholarships through institutions of higher education, including community colleges,

that are designated as National Centers of Academic Excellence in cybersecurity by the Department, to students who are enrolled in programs of study at such institutions leading to degrees or specialized program certifications in the cybersecurity field;

''(2) provide scholarship recipients with summer internship opportunities or other meaningful temporary appointments relating to the cybersecurity mission of the Department; and

''(3) prioritize the employment placement in the Department of at least 80 percent of scholarship recipients.

''(c) AMOUNT.—A scholarship awarded under the program shall be in an amount that—

''(1) covers the recipient's tuition and fees for not more than 4 years; and

''(2) provides the recipient with a stipend.

''(d) POST-AWARD EMPLOYMENT OBLIGATIONS.—Each scholarship recipient, as a condition of receiving a scholarship under the program, shall enter into an agreement under which the recipient agrees to work for a period of five years in the cybersecurity mission of the Department after receipt of the student's degree or specialized program certification in the cybersecurity field.

1 ''(e) ELIGIBILITY.— To be eligible to receive a schol-
2 arship under the program, an individual shall—
3 ''(1) be a citizen or lawful permanent resident
4 of the United States;
5 ''(2) have demonstrated a high level of com-
6 petency in relevant knowledge, skills, and abilities,
7 as defined by the national cybersecurity awareness
8 and education program of the National Institute of
9 Standards and Technology pursuant to section 401
10 of the Cybersecurity Enhancement Act of 2014 (15
11 U.S.C. 7451);
12 ''(3) be a full-time student in a technology-re-
13 lated degree program at an institution described in
14 subsection (b)(1), except that in the case of a stu-
15 dent who is enrolled in a community college, be a
16 student pursuing a degree on a less than full-time
17 basis, but not less than half-time basis; and
18 ''(4) accept the terms of a scholarship under
19 the program.
20 ''(f) CONDITIONS OF SUPPORT.—
21 ''(1) IN GENERAL.—As a condition of receiving
22 a scholarship under the program, a recipient shall
23 agree to provide the institution described in sub-
24 section (b)(1) with annual verifiable documentation

of post-award employment and up-to-date contact information.

"(2) TERMS.—A scholarship recipient under the program shall be liable to the United States as provided in subsection (i) if the recipient—

"(A) does not maintain an acceptable level of academic standing at the applicable institution described in subsection (b)(1), as determined by the Secretary, acting through the Director;

"(B) is dismissed for disciplinary reasons from such applicable institution;

"(C) withdraws from the eligible degree program before completing the program of study;

"(D) declares an intention to not fulfill the post-award employment obligation under the program; or

"(E) does not fulfill the post-award employment obligation under the program.

"(g) AMOUNT OF REPAYMENT.—

"(1) LESS THAN ONE YEAR OF SERVICE.—If a circumstance described in subsection (f)(2) occurs before the completion of one year of a post-award employment obligation under the program, the total

monetary amount of the scholarship award received by the recipient under the program shall be—

"(A) repaid; or

"(B) treated as a loan to be repaid in accordance with subsection (h).

"(2) ONE OR MORE YEARS OF SERVICE.—If a circumstance described in subparagraph (D) or (E) of subsection (f)(2) occurs after the completion of one or more years of a post-award employment obligation under the program, the total monetary amount of the scholarship awards received by the recipient under the program, reduced by the ratio of the number of years of service completed divided by the number of years of service required, shall be—

"(A) repaid; or

"(B) treated as a loan to be repaid in accordance with subsection (h).

"(h) REPAYMENTS.—A loan described in subsection (g) shall be—

"(1) treated as a Federal Direct Unsubsidized Stafford Loan under part D of title IV of the Higher Education Act of 1965 (20 U.S.C. 1087a et seq.); and

"(2) subject to repayment, together with interest thereon accruing from the date of the scholarship

award, in accordance with terms and conditions specified by the Secretary, acting through the Director, (in consultation with the Secretary of Education) in regulations promulgated to carry out this subsection.

''(i) COLLECTION OF REPAYMENT.—

''(1) IN GENERAL.—In the event that a scholarship recipient is required to repay the scholarship award under this section, an institution described in subsection (b)(1) providing the scholarship shall—

''(A) determine the repayment amounts and notify the recipient and the Secretary of the amounts owed; and

''(B) collect the repayment amounts within a period of time as determined by the Secretary, or the repayment amounts shall be treated as a loan in accordance with subsection (h).

''(2) RETURNED TO TREASURY.—Except as provided in paragraph (3), any repayment under this subsection shall be returned to the Treasury of the United States.

''(3) RETAINED PERCENTAGE.—An institution described in subsection (b)(1) may retain a percentage of any repayment such institution collects under

this subsection to defray administrative costs associated with such collection. The Secretary shall establish a single, fixed percentage that will apply to all such institutions.

''(j) EXCEPTIONS.—The Secretary may provide for the partial or total waiver or suspension of any service or repayment obligation by an individual under this section whenever compliance by such individual with such obligation is impossible or would involve extreme hardship to such individual, or if enforcement of such obligation with respect to such individual would be unconscionable.''.

(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 2218, as added by this title, the following new item:

''Sec. 2219. Scholarship for service.''.

SEC. 315. CYBERSECURITY AND INFRASTRUCTURE SECURITY AGENCY REVIEW.

(a) IN GENERAL.—The Director of the Cybersecurity and Infrastructure Security Agency of the Department of Homeland Security shall conduct a review of the ability of the Cybersecurity and Infrastructure Security Agency to carry out its mission requirements, as well as the recommendations detailed in the U.S. Cyberspace Solarium Commission's Report regarding the Agency.

(b) ELEMENTS OF REVIEW.—The review conducted in accordance with subsection (a) shall include the following elements:

(1) An assessment of how additional budget resources could be used by the Cybersecurity and Infrastructure Security Agency for projects and programs that—

(A) support the national risk management mission;

(B) support public and private-sector cybersecurity;

(C) promote public-private integration; and

(D) provide situational awareness of cybersecurity threats.

(2) A force structure assessment of the Cybersecurity and Infrastructure Security Agency, including—

(A) a determination of the appropriate size and composition of personnel to carry out the mission requirements of the Agency, as well as the recommendations detailed in the U.S. Cyberspace Solarium Commission's Report regarding the Agency;

(B) as assessment of whether existing personnel are appropriately matched to the

1 prioritization of threats in the cyber domain
2 and risks to critical infrastructure;
3 (C) an assessment of whether the Agency
4 has the appropriate personnel and resources
5 to—
6 (i) perform risk assessments, threat
7 hunting, and incident response to support
8 both private and public cybersecurity;
9 (ii) carry out its responsibilities re-
10 lated to the security of Federal information
11 and Federal information systems (as such
12 term is defined in section 3502 of title 44,
13 United States Code); and
14 (iii) carry out its critical infrastruc-
15 ture responsibilities, including national risk
16 management;
17 (D) an assessment of whether current
18 structure, personnel, and resources of regional
19 field offices are sufficient to carry out Agency
20 responsibilities and mission requirements; and
21 (E) an assessment of current Cybersecu-
22 rity and Infrastructure Security Agency facili-
23 ties, including a review of the suitability of such
24 facilities to fully support current and projected
25 mission requirements nationally and regionally,

and recommendations regarding future facility requirements.

(c) SUBMISSION OF REVIEW.—Not later than one year after the date of the enactment of this Act, the Secretary 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 detailing the result of the review conducted in accordance with subsection (a), including recommendations to address any identified gaps.

(d) GENERAL SERVICES ADMINISTRATION REVIEW.—

(1) SUBMISSION OF ASSESSMENT.—Upon submission to the Committee on Homeland Security of the House of Representatives and the Committee on Homeland Security and Governmental Affairs of the Senate of the report required under subsection (c), the Director of the Cybersecurity and Infrastructure Security Agency of the Department of Homeland Security shall submit to the Administrator of the General Services Administration the results of the assessment required under subsection (b)(2)(E).

(2) REVIEW.—The Administrator of the General Services Administration shall—

(A) conduct a review of Cybersecurity and Infrastructure Security Agency assessment required under subsection (b)(2)(E); and

(B) make recommendations regarding resources needed to procure or build a new facility or augment existing facilities to ensure sufficient size and accommodations to fully support current and projected mission requirements, including the integration of personnel from the private sector and other Federal departments and agencies.

(3) SUBMISSION OF REVIEW.—Not later than 30 days after receipt of the assessment in accordance with paragraph (1), the Administrator of the General Services Administration shall submit to the President, the Secretary of Homeland Security, the Committee on Homeland Security and Governmental Affairs of the Senate, and the Committee on Homeland Security of the House of Representatives the review required under paragraph (2).

SEC. 316. STRATEGY TO SECURE EMAIL.

(a) IN GENERAL.—Not later than December 31, 2021, the Secretary of Homeland Security shall develop and submit to Congress a strategy, including recommendations, to implement across all United States-

1 based email providers Domain-based Message Authentica-
2 tion, Reporting, and Conformance standard at scale.
3 (b) ELEMENTS.—The strategy required under sub-
4 section (a) shall include the following:
5 (1) A recommendation for the minimum size
6 threshold for United States-based email providers
7 for applicability of Domain-based Message Authen-
8 tication, Reporting, and Conformance.
9 (2) A description of the security and privacy
10 benefits of implementing the Domain-based Message
11 Authentication, Reporting, and Conformance stand-
12 ard at scale, including recommendations for national
13 security exemptions, as appropriate, as well as the
14 burdens of such implementation and an identifica-
15 tion of the entities on which such burdens would
16 most likely fall.
17 (3) An identification of key United States and
18 international stakeholders associated with such im-
19 plementation.
20 (4) An identification of any barriers to such im-
21 plementing, including a cost-benefit analysis where
22 feasible.
23 (5) An initial estimate of the total cost to the
24 Federal Government and implementing entities in
25 the private sector of such implementing, including

recommendations for defraying such costs, if applicable.

(c) CONSULTATION.—In developing the strategies and recommendations under subsection (a), the Secretary of Homeland Security may, as appropriate, consult with representatives from the information technology sector.

(d) EXEMPTION.—The Federal Advisory Committee Act (5 U.S.C. App.) shall not apply to this section or to any action to implement this section.

(e) DEFINITION.—In this section, the term ''Domain-based Message Authentication, Reporting, and Conformance'' means an email authentication, policy, and reporting protocol that verifies the authenticity of the sender of an email and blocks and reports to the sender fraudulent accounts.

SEC. 317. STRENGTHENING FEDERAL NETWORKS.

(a) AUTHORITY.—Section 3553(b) of title 44, United States Code, is amended—

(1) in paragraph (6)(D), by striking ''; and'' at the end and inserting a semicolon;

(2) by redesignating paragraph (7) as paragraph (8); and

(3) by inserting after paragraph (6) the following new paragraph:

"(7) hunting for and identifying, with or without advance notice, threats and vulnerabilities within Federal information systems; and".

(b) BINDING OPERATIONAL DIRECTIVE.—Not later than 1 year after the date of the enactment of this section, the Secretary of Homeland Security shall issue a binding operational directive pursuant to subsection (b)(2) of section 3553 of title 44, United States Code, to implement paragraph (7) of section 3553(b) of title 44, United States Code, as added by subsection (a).

SEC. 318. AUTHORIZATION OF APPROPRIATIONS.

For necessary expenses of the Cybersecurity and Infrastructure Security Agency of the Department of Homeland Security, including to carry out this title and the amendments made by this title, there is authorized to be appropriated to the Agency the following:

(1) $2,400,000,000 for fiscal year 2021.

(2) $2,800,000,000 for fiscal year 2022.

TITLE IV—BORDER AND VISA SECURITY

SEC. 401. ADDITIONAL U.S. CUSTOMS AND BORDER PROTECTION AGENTS AND OFFICERS.

(a) U.S. BORDER PATROL AGENTS AND PROCESSING COORDINATORS.—Not later than September 30, 2024, the Commissioner of U.S. Customs and Border Protection

shall hire, train, and assign sufficient U.S. Border Patrol personnel to maintain an active duty presence of not fewer than 26,370 full-time equivalent agents and not fewer than 1,200 processing coordinators.

(b) CBP OFFICERS.—Not later than September 30, 2024, the Commissioner of U.S. Customs and Border Protection shall hire, train, and assign sufficient U.S. Customs and Border Protection officers to maintain an active duty presence of not fewer than 27,725 full-time equivalent officers.

(c) AIR AND MARINE OPERATIONS.—Not later than September 30, 2024, the Commissioner of U.S. Customs and Border Protection shall hire, train, and assign sufficient agents for Air and Marine Operations of U.S. Customs and Border Protection to maintain not fewer than 1,675 full-time equivalent agents and not fewer than 264 Marine and Air Interdiction Agents for southern border air and maritime operations.

(d) PROFESSIONAL SUPPORT STAFF.—Not later than September 30, 2024, the Secretary of Homeland Security shall hire, train, and assign sufficient professional support staff for the recruitment, hiring, training, and maintenance of the personnel authorized under subsections (a) through (c).

(e) GAO REPORT.—If the staffing levels required under this section are not achieved by September 30, 2024, the Comptroller General of the United States shall conduct a review of the reasons why such levels were not achieved.

(f) AUTHORIZATION OF APPROPRIATIONS.—There is authorized to be appropriated $1,250,000,000 for each of fiscal years 2021 through 2024 to carry out subsection (a) though (d).

SEC. 402. ESTABLISHMENT OF WORKLOAD STAFFING MODELS FOR U.S. BORDER PATROL AND AIR AND MARINE OPERATIONS OF CBP.

(a) IN GENERAL.—Not later than one year after the date of the enactment of this Act, the Commissioner of U.S. Customs and Border Protection, in coordination with the Under Secretary for Management, the Chief Human Capital Officer, and the Chief Financial Officer of the Department of Homeland Security, shall implement a workload staffing model for each of the following:

(1) The U.S. Border Patrol.

(2) Air and Marine Operations of U.S. Customs and Border Protection.

(b) RESPONSIBILITIES OF THE COMMISSIONER OF CBP.—Subsection (c) of section 411 of the Homeland Security Act of 2002 (6 U.S.C. 211), is amended—

(1) by redesignating paragraphs (18) and (19) as paragraphs (20) and (21), respectively; and

(2) by inserting after paragraph (17) the following new paragraphs:

''(18) implement a staffing model that includes consideration for essential frontline operator activities and functions, variations in operating environments, present and planned infrastructure, present and planned technology, and required operations support levels for the U.S. Border Patrol, Air and Marine Operations, and the Office of Field Operations, to manage and assign personnel of such entities to ensure field and support posts possess adequate resources to carry out duties specified in this section;

''(19) develop standard operating procedures for a workforce tracking system within the U.S. Border Patrol, Air and Marine Operations, and the Office of Field Operations, train the workforce of each of such entities on the use, capabilities, and purpose of such system, and implement internal controls to ensure timely and accurate scheduling and reporting of actual completed work hours and activities;''.

(c) REPORT.—Not later than one year after the date of the enactment of this Act with respect to subsection (a) and paragraphs (18) and (19) of section 411(c) of the Homeland Security Act of 2002 (as amended by subsection (b)), and annually thereafter with respect to such paragraphs (18) and (19), the Secretary 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 status update on the implementation of such subsection (a) and such paragraphs (18) and (19), and status updates on such paragraphs (18) and (19), as well as all relevant workload staffing models. Such status updates shall include information on data sources and methodology used to generate such staffing models.

(d) INSPECTOR GENERAL REVIEW.—Not later than 120 days after the Commissioner of U.S. Customs and Border Protection develops a workload staffing model pursuant to subsection (a), the Inspector General of the Department of Homeland Security shall review such model and provide feedback to the Secretary of Homeland Security and the Committee on Homeland Security of the House of Representatives and the Committee on Homeland Security and Governmental Affairs of the Senate regarding the degree to which such model is responsive to

Inspector General recommendations, including recommendations from the Inspector General's February 2019 audit, and as appropriate, any further recommendations to improve such model.

SEC. 403. U.S. CUSTOMS AND BORDER PROTECTION RETENTION INCENTIVES.

(a) IN GENERAL.—Chapter 97 of title 5, United States Code, is amended by adding at the end the following:

"§ 9702. U.S. Customs and Border Protection temporary employment authorities

''(a) DEFINITIONS.—In this section—

''(1) the term 'CBP employee' means an employee of U.S. Customs and Border Protection;

''(2) the term 'Commissioner' means the Commissioner of U.S. Customs and Border Protection;

''(3) the term 'Director' means the Director of the Office of Personnel Management;

''(4) the term 'Secretary' means the Secretary of Homeland Security; and

''(5) the term 'appropriate congressional committees' means the Committee on Oversight and Reform, the Committee on Homeland Security, and the Committee on Ways and Means of the House of Representatives, and the Committee on Homeland

Security and Governmental Affairs and the Committee on Finance of the Senate.

"(b) DIRECT HIRE AUTHORITY; RECRUITMENT AND RELOCATION BONUSES; RETENTION BONUSES.—

"(1) DIRECT HIRE AUTHORITY.—The Secretary may appoint, without regard to sections 3309 through 3319, candidates to positions in the competitive service within U.S. Customs and Border Protection if the Secretary has given public notice of such positions before making any such appointment.

"(2) RECRUITMENT AND RELOCATION BONUSES.—The Secretary may pay a recruitment or relocation bonus of up to 50 percent of the annual rate of basic pay to an individual CBP employee as of the first day of the applicable service period (as prescribed by a written service agreement described in subparagraph (B)) multiplied by the number of years (including a fractional part of a year) in the service period if—

"(A) the Secretary determines that conditions consistent with the conditions described in paragraphs (1) and (2) of subsection (b) of section 5753 are satisfied with respect to the individual (without regard to the regulations referenced in subsection (b)(2)(B)(ii)(I)); and

1 ''(B) the individual enters into a written
2 service agreement with the Secretary—
3 ''(i) under which the individual is re-
4 quired to complete a period of employment
5 as a CBP employee of not less than 2
6 years; and
7 ''(ii) that includes—
8 ''(I) the commencement and ter-
9 mination dates of the required service
10 period (or provisions for the deter-
11 mination thereof);
12 ''(II) the amount of the bonus;
13 and
14 ''(III) other terms and conditions
15 under which the bonus is payable,
16 subject to the requirements of this
17 subsection, including—
18 ''(aa) the conditions under
19 which the agreement may be ter-
20 minated before the agreed-upon
21 service period has been com-
22 pleted; and
23 ''(bb) the effect of a termi-
24 nation described in item (aa).

1 "(3) RETENTION BONUSES.—The Secretary
2 may pay a retention bonus of up to 50 percent of
3 the annual rate of basic pay to an individual CBP
4 employee if—
5 "(A) the Secretary determines that—
6 "(i) a condition consistent with the
7 condition described in subsection (b)(1) of
8 section 5754 is satisfied with respect to the
9 CBP employee;
10 "(ii) in the absence of a retention
11 bonus, the CBP employee would be likely
12 to leave—
13 "(I) the Federal service; or
14 "(II) for a different position in
15 the Federal service, including a posi-
16 tion in another agency or component
17 of the Department of Homeland Secu-
18 rity; and
19 "(B) the CBP employee enters into a writ-
20 ten service agreement with the Secretary—
21 "(i) under which the employee is re-
22 quired to complete a period of employment
23 as a CBP employee of not less than 2
24 years; and
25 "(ii) that includes—

"(I) the commencement and termination dates of the required service period (or provisions for the determination thereof);

"(II) the amount of the bonus; and

"(III) other terms and conditions under which the bonus is payable, subject to the requirements of this subsection, including—

"(aa) the conditions under which the agreement may be terminated before the agreed-upon service period has been completed; and

"(bb) the effect of a termination described in item (aa).

"(4) RULES FOR BONUSES.—

"(A) MAXIMUM BONUS LIMITATIONS.—

"(i) UNDER PARAGRAPH (2).—A CBP employee may not receive a total amount of bonuses under paragraph (2) in excess of 100 percent of the annual rate of basic pay of the employee as of the first day of the applicable service period.

"(ii) UNDER PARAGRAPH (3).—A bonus paid to any CBP employee under paragraph (3) may not exceed 50 percent of the annual rate of basic pay of the employee.

"(B) RELATIONSHIP TO BASIC PAY.—A bonus paid under paragraph (2) or (3) shall not be considered part of the basic pay of the CBP employee for any purpose, including for retirement or in computing a lump-sum payment to the covered employee for accumulated and accrued annual leave under section 5551 or section 5552.

"(C) PERIOD OF SERVICE FOR RECRUITMENT, RELOCATION, AND RETENTION BONUSES.—

"(i) RESTRICTION.—A bonus paid under paragraph (3) may not be based on any period of such service which is the basis for a recruitment or relocation bonus under paragraph (2).

"(ii) FURTHER RESTRICTION.—A bonus paid under paragraph (2) or (3) may not be based on any period of service which is the basis for a recruitment or re-

1 location bonus under section 5753 or a re-
2 tention bonus under section 5754.
3 ''(D) LIMITATIONS.—No bonus may be
4 paid—
5 ''(i) under paragraph (2) to any indi-
6 vidual described in section 5753(a)(2); or
7 ''(ii) under paragraph (3) to any indi-
8 vidual described in section 5754(a)(2).
9 ''(c) SPECIAL RATES OF PAY.—In addition to the cir-
10 cumstances described in subsection (b) of section 5305,
11 the Director of the Office of Personnel Management may
12 establish special rates of pay in accordance with that sec-
13 tion to assist the Secretary in meeting staffing levels as
14 described in section 401. The Director shall prioritize the
15 consideration of requests from the Secretary for such spe-
16 cial rates of pay and issue a decision as soon as prac-
17 ticable. The Secretary shall provide such information to
18 the Director as the Director deems necessary to evaluate
19 special rates of pay under this subsection.
20 ''(d) OPM OVERSIGHT.—
21 ''(1) IN GENERAL.—Not later than September
22 30 of each year that the authorities under sub-
23 sections (b) and (c) are in effect, the Secretary shall
24 provide a report to the Director on U.S. Customs
25 and Border Protection's use of such authorities. In

each report, the Secretary shall provide such information as the Director determines is appropriate to ensure appropriate use of authorities under such subsections. Each report shall also include an assessment of—

"(A) the impact of the use of authorities under subsections (b) and (c) on implementation of meeting staffing levels as described in section 401;

"(B) whether the authorities solved hiring and retention challenges at the agency, including at specific locations;

"(C) whether hiring and retention challenges still exist at the agency or specific locations; and

"(D) whether the Secretary needs to continue to use authorities provided under this section at the agency or at specific locations.

"(2) CONSIDERATION.—In compiling a report under paragraph (1), the Secretary shall consider—

"(A) whether any CBP employee accepted an employment incentive under subsection (b) and (c) and then transferred to a new location or left U.S. Customs and Border Protection; and

1 "(B) the length of time that each employee
2 identified under subparagraph (A) stayed at the
3 original location before transferring to a new lo-
4 cation or leaving U.S. Customs and Border
5 Protection.
6 "(3) SUBMISSION TO CONGRESS.—In addition
7 to the Director, the Secretary shall submit each re-
8 port required under this subsection to the appro-
9 priate congressional committees.
10 "(e) OPM ACTION.—
11 "(1) NOTIFICATION.—If the Director deter-
12 mines the Secretary has inappropriately used au-
13 thorities under subsection (b) or (c), the Director
14 shall notify the Secretary and the appropriate con-
15 gressional committees in writing.
16 "(2) PROHIBITION.—Upon receipt of a notifica-
17 tion under paragraph (1), the Secretary may not
18 make any new appointment or issue any new bonus
19 under subsection (b), or provide any CBP employee
20 with further special rates of pay, until the Director
21 has provided the Secretary and the appropriate con-
22 gressional committees a written notice stating the
23 Director is satisfied safeguards are in place to pre-
24 vent further inappropriate use.

1 "(3) APPLICATION.—The prohibition under
2 paragraph (2) shall not apply to any bonus under
3 subsection (b) due to a CBP employee pursuant to
4 written service agreement entered into before the
5 date of receipt of a notification under such para-
6 graph.
7 "(f) IMPROVING CBP HIRING AND RETENTION.—
8 "(1) TRAINING OF CBP HIRING OFFICIALS.—
9 Not later than 180 days after the date of the enact-
10 ment of this section, and in conjunction with the
11 Chief Human Capital Officer of the Department of
12 Homeland Security, the Secretary shall develop and
13 implement a strategy to improve the training regard-
14 ing hiring and human resources flexibilities (includ-
15 ing hiring and human resources flexibilities for loca-
16 tions in rural or remote areas) for all employees,
17 serving in agency headquarters or field offices, who
18 are involved in the recruitment, hiring, assessment,
19 or selection of candidates for locations in a rural or
20 remote area, as well as the retention of current em-
21 ployees.
22 "(2) ELEMENTS.—Elements of the strategy
23 under paragraph (1) shall include the following:
24 "(A) Developing or updating training and
25 educational materials on hiring and human re-

sources flexibilities for employees who are involved in the recruitment, hiring, assessment, or selection of candidates, as well as the retention of current employees.

''(B) Regular training sessions for personnel who are critical to filling open positions in rural or remote areas.

''(C) The development of pilot programs or other programs, as appropriate, consistent with authorities provided to the Secretary to address identified hiring challenges, including in rural or remote areas.

''(D) Developing and enhancing strategic recruiting efforts through the relationships with institutions of higher education, as defined in section 102 of the Higher Education Act of 1965 (20 U.S.C. 1002), veterans transition and employment centers, and job placement program in regions that could assist in filling positions in rural or remote areas.

''(E) Examination of existing agency programs on how to most effectively aid spouses and families of individuals who are candidates or new hires in a rural or remote area.

1 ''(F) Feedback from individuals who are
2 candidates or new hires at locations in a rural
3 or remote area, including feedback on the qual-
4 ity of life in rural or remote areas for new hires
5 and their families.
6 ''(G) Feedback from CBP employees, other
7 than new hires, who are stationed at locations
8 in a rural or remote area, including feedback on
9 the quality of life in rural or remote areas for
10 those CBP employees and their families.
11 ''(H) Feedback in the form of an exit
12 interview from CBP employees who have de-
13 cided to voluntarily leave the agency.
14 ''(I) Evaluation of Department of Home-
15 land Security internship programs and the use-
16 fulness of those programs in improving hiring
17 by the Secretary in rural or remote areas.
18 ''(3) EVALUATION.—
19 ''(A) IN GENERAL.—Not later than one
20 year after developing and implementing the
21 strategy under paragraph (1) and each of the
22 four years thereafter, the Secretary shall—
23 ''(i) evaluate the extent to which the
24 strategy developed and implemented under

such paragraph has improved the hiring and retention ability of the Secretary; and

"(ii) make any appropriate updates to the strategy under such paragraph.

"(B) INFORMATION.—The evaluation conducted under subparagraph (A) shall include the following:

"(i) Any reduction in the time taken by the Secretary to fill mission-critical positions, including in rural or remote areas.

"(ii) A general assessment of the impact of the strategy implemented under paragraph (1) on hiring challenges, including in rural or remote areas.

"(iii) Other information the Secretary determines relevant.

"(g) INSPECTOR GENERAL REVIEW.—Not later than two years after the date of the enactment of this section, the Inspector General of the Department of Homeland Security shall review the use of hiring and pay flexibilities under subsections (b) and (c) to determine whether the use of such flexibilities is helping the Secretary meet hiring and retention needs, including in rural and remote areas.

1 "(h) REPORT ON POLYGRAPH REQUESTS.—The Sec-
2 retary shall report to the appropriate congressional com-
3 mittees on the number of requests the Secretary receives
4 from any other Federal agency for the file of an applicant
5 for a position in U.S. Customs and Border Protection that
6 includes the results of a polygraph examination.
7 "(i) EXERCISE OF AUTHORITY.—
8 "(1) SOLE DISCRETION.—The exercise of au-
9 thority under subsection (b) shall be subject to the
10 sole and exclusive discretion of the Secretary (or the
11 Commissioner of U.S. Customs and Border Protec-
12 tion, as applicable under paragraph (2) of this sub-
13 section), notwithstanding chapter 71 and any collec-
14 tive bargaining agreement.
15 "(2) DELEGATION.—The Secretary may dele-
16 gate any authority under this section to the Com-
17 missioner.
18 "(j) RULE OF CONSTRUCTION.—Nothing in this sec-
19 tion may be construed to exempt the Secretary or the Di-
20 rector from applicability of the merit system principles
21 under section 2301.
22 "(k) SUNSET.—The authorities under subsections (b)
23 and (c) shall terminate on September 30, 2024. Any bonus
24 to be paid pursuant to subsection (b) that is approved be-

fore such date may continue until such bonus has been paid, subject to the conditions specified in this section.''.

(b) TECHNICAL AND CONFORMING AMENDMENT.—The table of sections for chapter 97 of title 5, United States Code, is amended by adding at the end the following new item:

''9702. U.S. Customs and Border Protection temporary employment authorities.''.

SEC. 404. STUDY ON EFFICACY OF CERTAIN PERSONNEL SCREENING METHODS FOR U.S. CUSTOMS AND BORDER PROTECTION USE.

(a) IN GENERAL.—Not later than 60 days after the date of the enactment of this Act, the Secretary of Homeland Security shall enter into an agreement with the National Academy of Sciences to conduct a study on the efficacy of certain personnel screening methods for U.S. Customs and Border Protection use. Such study shall include the following:

(1) A review of the appropriateness of the use of polygraph examinations in determining candidate suitability during the U.S. Customs and Border Protection hiring process.

(2) A cost-benefit analysis of using polygraph examinations for candidate suitability during the U.S. Customs and Border Protection hiring process.

(3) A review of research related to alternatives to polygraph examinations appropriate for use during the U.S. Customs and Border Protection hiring process.

(b) MATTERS INCLUDED.—The study required under subsection (a) shall—

(1) assess prior scientific, academic, and government literature on the topics described in such subsection;

(2) identify and examine assumptions about polygraph examinations that underlie the polygraph mandate under the Anti-Border Corruption Act of 2010 (Public Law 111–376); and

(3) provide specific recommendations related to—

(A) the future use of such polygraph examinations, including a consideration of whether such polygraph mandate aligns with current scientific evidence and offers a reliable indication of future susceptibility to corruption; and

(B) the appropriate alternative mechanisms or technology, including private sector tools, that could be used during the U.S. Customs and Border Protection hiring process to pre-screen for susceptibility to corruption; and

(4) provide any other recommendations the Secretary of Homeland Secretary determines relevant.

(c) SUBMISSION.—Not later than one year after the date of the enactment of this Act, the Secretary of the Homeland Security shall submit to the appropriate congressional committees the study required under subsection (a).

(d) DEFINITIONS.—In this section:

(1) APPROPRIATE CONGRESSIONAL COMMITTEES.—The term ''appropriate congressional committees'' means the Committee on Homeland Security of the House of Representatives and the Committee on Homeland Security and Governmental Affairs of the Senate.

(2) POLYGRAPH EXAMINATIONS.—The term ''polygraph examinations'' means polygraph examinations conducted in accordance with section 3(1) of the Anti-Border Corruption Act of 2010.

SEC. 405. HIRING FLEXIBILITY.

Section 3 of the Anti-Border Corruption Act of 2010 (Public Law 111–376; 6 U.S.C. 221) is amended by striking subsection (b) and inserting the following new subsections:

1 "(b) WAIVER AUTHORITY.—The Commissioner of
2 U.S. Customs and Border Protection may waive the appli-
3 cation of subsection (a)(1) in the following circumstances:
4 "(1) In the case of a current, full-time law en-
5 forcement officer employed by a State or local law
6 enforcement agency, if such officer—
7 "(A) has served as a law enforcement offi-
8 cer for not fewer than three years with no
9 break in service;
10 "(B) is authorized by law to engage in or
11 supervise the prevention, detection, investiga-
12 tion, or prosecution of, or the incarceration of
13 any person for, any violation of law, and has
14 statutory powers for arrest or apprehension;
15 "(C) is not currently under investigation,
16 has not been found to have engaged in criminal
17 activity or serious misconduct, has not resigned
18 from a law enforcement officer position under
19 investigation or in lieu of termination, and has
20 not been dismissed from a law enforcement offi-
21 cer position; and
22 "(D) has, within the past ten years, suc-
23 cessfully completed a polygraph examination,
24 described in subsection (c), as a condition of

1 employment with such officer's current law en-
2 forcement agency.
3 ''(2) In the case of a current, full-time law en-
4 forcement officer employed by a Federal law enforce-
5 ment agency, if such officer—
6 ''(A) has served as a law enforcement offi-
7 cer for not fewer than three years with no
8 break in service;
9 ''(B) has authority to make arrests, con-
10 duct investigations, conduct searches, make sei-
11 zures, carry firearms, and serve orders, war-
12 rants, and other processes;
13 ''(C) is not currently under investigation,
14 has not been found to have engaged in criminal
15 activity or serious misconduct, has not resigned
16 from a law enforcement officer position under
17 investigation or in lieu of termination, and has
18 not been dismissed from a law enforcement offi-
19 cer position; and
20 ''(D) holds a current background investiga-
21 tion to the level required for service as a law
22 enforcement officer with U.S. Customs and
23 Border Protection.

1 "(3) In the case of an individual who is a mem-
2 ber of the Armed Forces (or a reserve component
3 thereof) or a veteran, if such individual—
4 "(A) has served in the Armed Forces for
5 not fewer than three years;
6 "(B) holds, or has held within the past five
7 years, a Secret, Top Secret, or Top Secret/Sen-
8 sitive Compartmented Information clearance;
9 "(C) holds or has undergone and passed a
10 background investigation to the level required
11 for service as a law enforcement officer with
12 U.S. Customs and Border Protection;
13 "(D) received, or is eligible to receive, an
14 honorable discharge from service in the Armed
15 Forces and has not engaged in criminal activity
16 or committed a serious military or civil offense
17 under the Uniform Code of Military Justice;
18 and
19 "(E) was not granted any waivers to ob-
20 tain the clearance referred to subparagraph
21 (B).
22 "(c) CERTAIN POLYGRAPH EXAMINATION.—A poly-
23 graph examination described in this subsection is a poly-
24 graph examination that satisfies requirements established

by the Secretary of Homeland Security, in consultation with the Director of National Intelligence.

''(d) TERMINATION OF WAIVER AUTHORITY.—The authority to issue a waiver under subsection (b) shall terminate on the date that is five years after the date of the enactment of the Anti-Border Corruption Reauthorization Act of 2019.''.

SEC. 406. SUPPLEMENTAL COMMISSIONER AUTHORITY AND DEFINITIONS.

(a) SUPPLEMENTAL COMMISSIONER AUTHORITY.—Section 4 of the Anti-Border Corruption Act of 2010 (Public Law 111–376) is amended to read as follows:

''SEC. 4. SUPPLEMENTAL COMMISSIONER AUTHORITY.

''(a) NON-EXEMPTION.—An individual who receives a waiver under subsection (b) of section 3 shall not be exempt from other hiring requirements relating to suitability for employment and eligibility to hold a national security designated position, as determined by the Commissioner of U.S. Customs and Border Protection.

''(b) BACKGROUND INVESTIGATIONS.—Any individual who receives a waiver under subsection (b) of section 3 who holds a current background investigation may be subject to further background investigation to the level required for service as a law enforcement officer with U.S. Customs and Border Protection.

1 ''(c) CONTINUOUS EVALUATION.—Any individual
2 who receives a waiver under subsection (b) of section 3
3 shall not be exempt from any requirement relating to con-
4 tinuous evaluation established by the Commissioner of
5 U.S. Customs and Border Protection.

6 ''(d) ADMINISTRATION OF POLYGRAPH EXAMINA-
7 TION.—The Commissioner of U.S. Customs and Border
8 Protection is authorized to administer a polygraph exam-
9 ination to an applicant or employee who is eligible for or
10 receives a waiver under subsection (b) of section 3 if infor-
11 mation is discovered prior to the completion of a back-
12 ground investigation that results in a determination that
13 a polygraph examination is necessary to make a final de-
14 termination regarding suitability for employment or con-
15 tinued employment, as the case may be.''.

16 (b) REPORT.—The Anti-Border Corruption Act of
17 2010 is amended by adding at the end the following new
18 section:

19 **''SEC. 5. REPORTING.**

20 ''Not later than one year after the date of the enact-
21 ment of this section and every year for the next four years
22 thereafter, the Commissioner of U.S. Customs and Border
23 Protection shall provide the Committee on Homeland Se-
24 curity of the House of Representatives and the Committee
25 on Homeland Security and Governmental Affairs of the

Senate information on the number, disaggregated with respect to each of paragraphs (1), (2), and (3) of subsection (b) of section 3, of waivers requested, granted, and denied, and the reasons for any such denial, and the final outcome of the application for employment at issue. Such information shall also include the number of instances a polygraph examination was administered under the conditions described in subsection (d) of section 4, the result of such examination, and the final outcome of the application for employment at issue.''.

(c) DEFINITIONS.—The Anti-Border Corruption Act of 2010, as amended by subsection (b) of this section, is further amended by adding at the end the following new section:

"SEC. 6. DEFINITIONS.

''In this Act:

''(1) LAW ENFORCEMENT OFFICER.—The term 'law enforcement officer' has the meaning given such term in sections 8331(20) and 8401(17) of title 5, United States Code.

''(2) VETERAN.—The term 'veteran' has the meaning given such term in section 101(2) of title 38, United States Code.

"(3) SERIOUS MILITARY OR CIVIL OFFENSE.—The term 'serious military or civil offense' means an offense for which—

"(A) a member of the Armed Forces may be discharged or separated from service in the Armed Forces; and

"(B) a punitive discharge is, or would be, authorized for the same or a closely related offense under the Manual for Court-Martial, as pursuant to Army Regulation 635–200 chapter 14–12.".

SEC. 407. TECHNICAL AND CONFORMING AMENDMENT.

Paragraph (15) of section 411(c) of the Homeland Security Act of 2002 (6 U.S.C. 211(c)) is amended by striking "section 3(1)" and inserting "section 3".

SEC. 408. PORTS OF ENTRY INFRASTRUCTURE.

(a) ADDITIONAL PORTS OF ENTRY.—

(1) AUTHORITY.—The Administrator of General Services may, subject to section 3307 of title 40, United States Code, construct new ports of entry along the northern border and southern border at locations determined by the Secretary of Homeland Security.

(2) CONSULTATION.—

(A) REQUIREMENT TO CONSULT.—The Secretary of Homeland Security and the Administrator of General Services shall consult with the Secretary of State, the Secretary of the Interior, the Secretary of Agriculture, the Secretary of Transportation, and appropriate representatives of State and local governments, Tribes, and property owners in the United States prior to determining a location for any new port of entry constructed pursuant to paragraph (1).

(B) CONSIDERATIONS.—The purpose of the consultations required by subparagraph (A) shall be to minimize any negative impacts of constructing a new port of entry on the environment, culture, commerce, and quality of life of the communities and residents located near such new port.

(b) EXPANSION AND MODERNIZATION OF HIGH-PRIORITY SOUTHERN BORDER PORTS OF ENTRY.—Not later than September 30, 2025, the Administrator of General Services, subject to section 3307 of title 40, United States Code, and in coordination with the Secretary of Homeland Security, shall expand or modernize high-priority ports of entry on the southern border, as determined by the Sec-

1 retary and identified in section 430, for the purposes of
2 reducing wait times and enhancing security.
3 (c) PORT OF ENTRY PRIORITIZATION.—Prior to con-
4 structing any new ports of entry pursuant to subsection
5 (a), the Administrator of General Services shall complete
6 the expansion and modernization of ports of entry pursu-
7 ant to subsection (b) to the extent practicable.
8 (d) NOTIFICATIONS.—
9 (1) RELATING TO NEW PORTS OF ENTRY.—Not
10 later than 15 days after determining the location of
11 any new port of entry for construction pursuant to
12 subsection (a), the Secretary of Homeland Security
13 and the Administrator of General Services shall
14 jointly notify the Members of Congress who rep-
15 resent the State or congressional district in which
16 such new port of entry will be located, as well as the
17 Committee on Homeland Security and Governmental
18 Affairs, the Committee on Finance, the Committee
19 on Commerce, Science, and Transportation, and the
20 Committee on the Judiciary of the Senate, and the
21 Committee on Homeland Security, the Committee on
22 Ways and Means, the Committee on Transportation
23 and Infrastructure, and the Committee on the Judi-
24 ciary of the House of Representatives. Such notifica-
25 tion shall include information relating to the location

of such new port of entry, a description of the need for such new port of entry and associated anticipated benefits, a description of the consultations undertaken by the Secretary and the Administrator pursuant to paragraph (2) of such subsection, any actions that will be taken to minimize negative impacts of such new port of entry, and the anticipated time-line for construction and completion of such new port of entry.

(2) RELATING TO EXPANSION AND MODERNIZATION OF PORTS OF ENTRY.—Not later than 180 days after enactment of this Act, the Secretary of Homeland Security and the Administrator of General Services shall jointly notify the Committee on Homeland Security and Governmental Affairs, the Committee on Finance, the Committee on Commerce, Science, and Transportation, and the Committee on the Judiciary of the Senate, and the Committee on Homeland Security, the Committee on Ways and Means, the Committee on Transportation and Infrastructure, and the Committee on the Judiciary of the House of Representatives of the ports of entry on the southern border that are the subject of expansion or modernization pursuant to subsection (b) and the Secretary's and Administrator's

plan for expanding or modernizing each such port of entry.

(e) SAVINGS PROVISION.—Nothing in this section may be construed to—

(1) create or negate any right of action for a State, local government, or other person or entity affected by this section;

(2) delay the transfer of the possession of property to the United States or affect the validity of any property acquisitions by purchase or eminent domain, or to otherwise affect the eminent domain laws of the United States or of any State; or

(3) create any right or liability for any party.

(f) RULE OF CONSTRUCTION.—Nothing in this section may be construed as providing the Secretary of Homeland Security new authority related to the construction, acquisition, or renovation of real property.

SEC. 409. U.S. CUSTOMS AND BORDER PROTECTION TECHNOLOGY UPGRADES.

(a) SECURE COMMUNICATIONS.—The Commissioner of U.S. Customs and Border Protection shall ensure that each U.S. Customs and Border Protection officer or agent, if appropriate, is equipped with a secure radio or other two-way communication device, supported by system inter-

operability, that allows each such officer to communicate—

(1) between ports of entry and inspection stations; and

(2) with other Federal, State, Tribal, and local law enforcement entities.

(b) BORDER SECURITY DEPLOYMENT PROGRAM.—

(1) EXPANSION.—Not later than September 30, 2023, the Commissioner of U.S. Customs and Border Protection shall fully implement the Border Security Deployment Program of U.S. Customs and Border Protection and expand the integrated surveillance and intrusion detection system at land ports of entry along the southern border and the northern border.

(2) AUTHORIZATION OF APPROPRIATIONS.—In addition to amounts otherwise authorized to be appropriated for such purpose, there is authorized to be appropriated $33,000,000 for fiscal years 2021 and 2022 to carry out paragraph (1).

(c) UPGRADE OF LICENSE PLATE READERS AT PORTS OF ENTRY.—

(1) UPGRADE.—Not later than two years after the date of the enactment of this Act, the Commissioner of U.S. Customs and Border Protection shall

upgrade all existing license plate readers in need of upgrade, as determined by the Commissioner, on the northern and southern borders on incoming and outgoing vehicle lanes.

(2) AUTHORIZATION OF APPROPRIATIONS.—In addition to amounts otherwise authorized to be appropriated for such purpose, there is authorized to be appropriated $125,000,000 for fiscal years 2021 through 2022 to carry out paragraph (1).

(d) BIOMETRIC ENTRY-EXIT.—

(1) IN GENERAL.—Subtitle B of title IV of the Homeland Security Act of 2002 (6 U.S.C. 211 et seq.) is amended by adding at the end the following new section:

"SEC. 420. BIOMETRIC ENTRY-EXIT.

''(a) ESTABLISHMENT.—The Secretary shall—

''(1) not later than 180 days after the date of the enactment of this section, submit to the Committee on Homeland Security and the Committee on the Judiciary of the House of Representatives and the Committee on Homeland Security and Governmental Affairs and the Committee on the Judiciary of the Senate an implementation plan to establish a biometric exit data system to complete the integrated biometric entry and exit data system required

under section 7208 of the Intelligence Reform and Terrorism Prevention Act of 2004 (8 U.S.C. 1365b), including—

"(A) an integrated master schedule and cost estimate, including requirements and design, development, operational, and maintenance costs of such a system, that takes into account prior reports on such matters issued by the Government Accountability Office and the Department;

"(B) cost-effective staffing and personnel requirements of such a system that leverages existing resources of the Department that takes into account prior reports on such matters issued by the Government Accountability Office and the Department;

"(C) a consideration of training programs necessary to establish such a system that takes into account prior reports on such matters issued by the Government Accountability Office and the Department;

"(D) a consideration of how such a system will affect arrival and departure wait times that takes into account prior reports on such matter

issued by the Government Accountability Office and the Department;

''(E) a consideration of audit capability for systems procured in partnership with the private sector to achieve biometric exit;

''(F) information received after consultation with private sector stakeholders, including the—

''(i) trucking industry;

''(ii) airport industry;

''(iii) airline industry;

''(iv) seaport industry;

''(v) travel industry; and

''(vi) biometric technology industry;

''(G) a consideration of how trusted traveler programs in existence as of the date of the enactment of this section may be impacted by, or incorporated into, such a system;

''(H) defined metrics of success and milestones;

''(I) identified risks and mitigation strategies to address such risks;

''(J) a consideration of how other countries have implemented a biometric exit data system;

1 "(K) a consideration of stakeholder privacy
2 concerns; and
3 "(L) a list of statutory, regulatory, or ad-
4 ministrative authorities, if any, needed to inte-
5 grate such a system into the operations of the
6 Transportation Security Administration; and
7 "(2) not later than two years after the date of
8 the enactment of this section, establish a biometric
9 exit data system at the—
10 "(A) 15 United States airports that sup-
11 port the highest volume of international air
12 travel, as determined by available Federal flight
13 data;
14 "(B) 10 United States seaports that sup-
15 port the highest volume of international sea
16 travel, as determined by available Federal travel
17 data; and
18 "(C) 15 United States land ports of entry
19 that support the highest volume of vehicle, pe-
20 destrian, and cargo crossings, as determined by
21 available Federal border crossing data.
22 "(b) IMPLEMENTATION.—
23 "(1) PILOT PROGRAM AT LAND PORTS OF
24 ENTRY.—Not later than six months after the date of
25 the enactment of this section, the Secretary, in col-

1 laboration with industry stakeholders, shall establish
2 a six-month pilot program to test the biometric exit
3 data system referred to in subsection (a)(2) on non-
4 pedestrian outbound traffic at not fewer than three
5 land ports of entry with significant cross-border traf-
6 fic, including at not fewer than two land ports of
7 entry on the southern land border and at least one
8 land port of entry on the northern land border. Such
9 pilot program may include a consideration of more
10 than one biometric mode, and shall be implemented
11 to determine the following:
12 ''(A) How a nationwide implementation of
13 such biometric exit data system at land ports of
14 entry shall be carried out.
15 ''(B) The infrastructure required to carry
16 out subparagraph (A).
17 ''(C) The effects of such pilot program on
18 legitimate travel and trade.
19 ''(D) The effects of such pilot program on
20 wait times, including processing times, for such
21 non-pedestrian traffic.
22 ''(E) The effects of such pilot program on
23 combating terrorism.

1 ''(F) The effects of such pilot program on
2 identifying visa holders who violate the terms of
3 their visas.
4 ''(2) AT LAND PORTS OF ENTRY.—
5 ''(A) IN GENERAL.—Not later than five
6 years after the date of the enactment of this
7 section, the Secretary shall expand the biomet-
8 ric exit data system referred to in subsection
9 (a)(2) to all land ports of entry.
10 ''(B) EXTENSION.—The Secretary may ex-
11 tend for a single two-year period the date speci-
12 fied in subparagraph (A) if the Secretary cer-
13 tifies to the Committee on Homeland Security
14 and Governmental Affairs and the Committee
15 on the Judiciary of the Senate and the Com-
16 mittee on Homeland Security and the Com-
17 mittee on the Judiciary of the House of Rep-
18 resentatives that the 15 land ports of entry that
19 support the highest volume of passenger vehi-
20 cles, as determined by available Federal data,
21 do not have the physical infrastructure or char-
22 acteristics to install the systems necessary to
23 implement a biometric exit data system. Such
24 extension shall apply only in the case of non-pe-

1 destrian outbound traffic at such land ports of
2 entry.
3 ''(3) AT AIR AND SEA PORTS OF ENTRY.—Not
4 later than five years after the date of the enactment
5 of this section, the Secretary shall expand the bio-
6 metric exit data system referred to in subsection
7 (a)(2) to all air and sea ports of entry.
8 ''(c) EFFECTS ON AIR, SEA, AND LAND TRANSPOR-
9 TATION.—The Secretary, in consultation with appropriate
10 private sector stakeholders, shall ensure that the collection
11 of biometric data under this section causes the least pos-
12 sible disruption to the movement of people or cargo in air,
13 sea, or land transportation, while fulfilling the goals of im-
14 proving counterterrorism efforts and identifying visa hold-
15 ers who violate the terms of their visas.
16 ''(d) TERMINATION OF PROCEEDING.—Notwith-
17 standing any other provision of law, the Secretary shall,
18 on the date of the enactment of this section, terminate
19 the proceeding entitled 'Collection of Alien Biometric Data
20 Upon Exit From the United States at Air and Sea Ports
21 of Departure; United States Visitor and Immigrant Status
22 Indicator Technology Program (''US–VISIT'')', issued on
23 April 24, 2008 (73 Fed. Reg. 22065).
24 ''(e) DATA-MATCHING.—The biometric exit data sys-
25 tem established under this section shall—

"(1) match biometric information for an individual, regardless of nationality, citizenship, or immigration status, who is departing the United States against biometric data previously provided to the United States Government by such individual for the purposes of international travel;

"(2) leverage the infrastructure and databases of the current biometric entry and exit system established pursuant to section 7208 of the Intelligence Reform and Terrorism Prevention Act of 2004 (8 U.S.C. 1365b) for the purpose described in paragraph (1); and

"(3) be interoperable with, and allow matching against, other Federal databases that—

"(A) store biometrics of known or suspected terrorists; and

"(B) identify visa holders who violate the terms of their visas.

"(f) SCOPE.—

"(1) IN GENERAL.—The biometric exit data system established under this section shall include a requirement for the collection of biometric exit data at the time of departure for all categories of individuals who are required by the Secretary to provide biometric entry data.

"(2) EXCEPTION FOR CERTAIN OTHER INDIVIDUALS.—This section shall not apply in the case of an individual who exits and then enters the United States on a passenger vessel (as such term is defined in section 2101 of title 46, United States Code) the itinerary of which originates and terminates in the United States.

"(3) EXCEPTION FOR LAND PORTS OF ENTRY.—This section shall not apply in the case of a United States or Canadian citizen who exits the United States through a land port of entry.

"(g) COLLECTION OF DATA.—The Secretary may not require any non-Federal person to collect biometric data, or contribute to the costs of collecting or administering the biometric exit data system established under this section, except through a mutual agreement.

"(h) MULTI-MODAL COLLECTION.—In carrying out subsections (a)(1) and (b), the Secretary shall make every effort to collect biometric data using multiple modes of biometrics.

"(i) FACILITIES.—All facilities at which the biometric exit data system established under this section is implemented shall provide and maintain space for Federal use that is adequate to support biometric data collection and other inspection-related activity. For non-federally owned

1 facilities, such space shall be provided and maintained at
2 no cost to the Government. For all facilities at land ports
3 of entry, such space requirements shall be coordinated
4 with the Administrator of General Services.

5 ''(j) NORTHERN LAND BORDER.—In the case of the
6 northern land border, the requirements under subsections
7 (a)(2)(C), (b)(2)(A), and (b)(4) may be achieved through
8 the sharing of biometric data provided to the Department
9 by the Canadian Border Services Agency pursuant to the
10 2011 Beyond the Border agreement.

11 ''(k) FULL AND OPEN COMPETITION.—The Sec-
12 retary shall procure goods and services to implement this
13 section through full and open competition in accordance
14 with the Federal Acquisition Regulations.

15 ''(l) OTHER BIOMETRIC INITIATIVES.—Nothing in
16 this section may be construed as limiting the authority of
17 the Secretary to collect biometric information in cir-
18 cumstances other than as specified in this section.

19 ''(m) CONGRESSIONAL REVIEW.—Not later than 90
20 days after the date of the enactment of this section, the
21 Secretary shall submit to the Committee on Homeland Se-
22 curity and Governmental Affairs of the Senate, the Com-
23 mittee on the Judiciary of the Senate, the Committee on
24 Homeland Security of the House of Representatives, and
25 Committee on the Judiciary of the House of Representa-

1 tives reports and recommendations regarding the Science
2 and Technology Directorate's Air Entry and Exit Re-En-
3 gineering Program of the Department and the U.S. Cus-
4 toms and Border Protection entry and exit mobility pro-
5 gram demonstrations.

6 ''(n) SAVINGS CLAUSE.—Nothing in this section may
7 prohibit the collection of user fees permitted by section
8 13031 of the Consolidated Omnibus Budget Reconciliation
9 Act of 1985 (19 U.S.C. 58c).''.

10 (2) AUTHORIZATION OF APPROPRIATIONS.—
11 There is authorized to be appropriated $50,000,000
12 for each of fiscal years 2021 and 2022 to carry out
13 section 420 of the Homeland Security Act of 2002,
14 as added by this subsection.

15 (e) CLERICAL AMENDMENT.—The table of contents
16 in section 1(b) of the Homeland Security Act of 2002 is
17 amended by inserting after the item relating to section
18 419 the following new item:

''Sec. 420. Biometric entry-exit.''.

19 **SEC. 410. PHYSICAL BARRIERS ALONG THE SOUTHWEST**
20 **BORDER.**

21 Section 102 of the Illegal Immigration Reform and
22 Immigrant Responsibility Act of 1996 (Division C of Pub-
23 lic Law 104–208; 8 U.S.C. 1103 note) is amended—

24 (1) by amending subsection (a) to read as fol-
25 lows:

1 ''(a) IN GENERAL.—The Secretary of Homeland Se-
2 curity shall take such actions as may be necessary (includ-
3 ing the removal of obstacles to detection of illegal en-
4 trants) to design, test, construct, install, deploy, integrate,
5 and operate physical barriers, tactical infrastructure, and
6 technology in the vicinity of the United States border to
7 achieve situational awareness and operational control of
8 the border and deter, impede, and detect illegal activity.'';
9 (2) in subsection (b)—
10 (A) in the subsection heading, by striking
11 ''FENCING AND ROAD IMPROVEMENTS'' and in-
12 serting ''PHYSICAL BARRIERS'';
13 (B) in paragraph (1)—
14 (i) in subparagraph (A)—
15 (I) by striking ''subsection (a)''
16 and inserting ''this section'';
17 (II) by striking ''roads, lighting,
18 cameras, and sensors'' and inserting
19 ''tactical infrastructure, and tech-
20 nology''; and
21 (III) by striking ''gain'' inserting
22 ''achieve situational awareness and'';
23 and
24 (ii) by amending subparagraph (B) to
25 read as follows:

"(B) PHYSICAL BARRIERS AND TACTICAL INFRASTRUCTURE.—

"(i) IN GENERAL.—Not later than September 30, 2023, the Secretary of Homeland Security, in carrying out this section, shall deploy along the United States border the most practical and effective physical barriers and tactical infrastructure available for achieving situational awareness and operational control of the border.

"(ii) CONSIDERATION FOR CERTAIN PHYSICAL BARRIERS AND TACTICAL INFRASTRUCTURE.—The deployment of physical barriers and tactical infrastructure under this subparagraph shall not apply in any area or region along the border where natural terrain features, natural barriers, or the remoteness of such area or region would make any such deployment ineffective, as determined by the Secretary, for the purposes of achieving situational awareness or operational control of such area or region.";

(iii) in subparagraph (C)—

(I) by amending clause (i) to read as follows:

"(i) IN GENERAL.—In carrying out this section, the Secretary of Homeland Security shall consult with the Secretary of the Interior, the Secretary of Agriculture, appropriate representatives of Federal, State, local, and tribal governments, and appropriate private property owners in the United States to minimize the impact on the environment, culture, commerce, and quality of life for the communities and residents located near the sites at which such physical barriers are to be constructed.";

(II) in clause (ii)—

(aa) in subclause (I), by striking "or" after the semicolon at the end;

(bb) by amending subclause (II) to read as follows:

"(II) delay the transfer of the possession of property to the United States or affect the validity of any property acquisition by purchase or

eminent domain, or to otherwise affect the eminent domain laws of the United States or of any State; or''; and

(cc) by adding at the end the following new subclause:

''(III) create any right or liability for any party.''; and

(iv) by striking subparagraph (D);

(C) in paragraph (2)—

(i) by striking ''Attorney General'' and inserting ''Secretary of Homeland Security'';

(ii) by striking ''this subsection'' and inserting ''this section''; and

(iii) by striking ''construction of fences'' and inserting ''the construction of physical barriers'';

(D) by amending paragraph (3) to read as follows:

''(3) AGENT SAFETY.—In carrying out this section, the Secretary of Homeland Security, when designing, constructing, and deploying physical barriers, tactical infrastructure, or technology, shall incorporate such safety features into such design, con-

1 struction, or deployment of such physical barriers,
2 tactical infrastructure, or technology, as the case
3 may be, that the Secretary determines, in the Sec-
4 retary's sole discretion, are necessary to maximize
5 the safety and effectiveness of officers or agents of
6 the Department of Homeland Security or of any
7 other Federal agency deployed in the vicinity of such
8 physical barriers, tactical infrastructure, or tech-
9 nology.''; and
10 (E) in paragraph (4), by striking ''this
11 subsection'' and inserting ''this section'';
12 (3) in subsection (c), by amending paragraph
13 (1) to read as follows:
14 ''(1) IN GENERAL.—Notwithstanding any other
15 provision of law, the Secretary of Homeland Security
16 shall have the authority to waive all legal require-
17 ments the Secretary, in the Secretary's sole discre-
18 tion, determines necessary to ensure the expeditious
19 design, testing, construction, installation, deploy-
20 ment, integration, and operation of the physical bar-
21 riers, tactical infrastructure, and technology under
22 this section. Such waiver authority shall also apply
23 with respect to any maintenance carried out on such
24 physical barriers, tactical infrastructure, or tech-
25 nology. Any such decision by the Secretary shall be

effective upon publication in the Federal Register.''; and

(4) by adding after subsection (d) the following new subsections:

''(e) TECHNOLOGY.—Not later than September 30, 2023, the Secretary of Homeland Security, in carrying out this section, shall deploy along the United States border the most practical and effective technology available for achieving situational awareness and operational control of the border.

''(f) DEFINITIONS.—In this section:

''(1) OPERATIONAL CONTROL.—The term 'operational control' has the meaning given such term in section 2(b) of the Secure Fence Act of 2006 (8 U.S.C. 1701 note; Public Law 109–367).

''(2) PHYSICAL BARRIERS.—The term 'physical barriers' includes reinforced fencing, border wall system, and levee walls.

''(3) SITUATIONAL AWARENESS.—The term 'situational awareness' has the meaning given such term in section 1092(a)(7) of the National Defense Authorization Act for Fiscal Year 2017 (6 U.S.C. 223(a)(7); Public Law 114–328).

1 "(4) TACTICAL INFRASTRUCTURE.—The term
2 'tactical infrastructure' includes boat ramps, access
3 gates, checkpoints, lighting, and roads.
4 "(5) TECHNOLOGY.—The term 'technology' in-
5 cludes border surveillance and detection technology,
6 including the following:
7 "(A) Tower-based surveillance technology.
8 "(B) Deployable, lighter-than-air ground
9 surveillance equipment.
10 "(C) Vehicle and Dismount Exploitation
11 Radars (VADER).
12 "(D) border tunnel detection technology.
13 "(E) Advanced unattended surveillance
14 sensors.
15 "(F) Mobile vehicle-mounted and man-
16 portable surveillance capabilities.
17 "(G) Unmanned aerial vehicles.
18 "(H) Other border detection, communica-
19 tions, and surveillance technology.
20 "(6) UNMANNED AERIAL VEHICLES.—The term
21 'unmanned aerial vehicle' has the meaning given the
22 term 'unmanned aircraft' in section 44801 of the
23 FAA Modernization and Reform Act of 2018 (Public
24 Law 115–254; 49 U.S.C. 40101 note).".

SEC. 411. AIR AND MARINE OPERATIONS FLIGHT HOURS.

(a) INCREASED FLIGHT HOURS.—The Secretary of Homeland Security shall ensure that not fewer than 95,000 annual flight hours are carried out by Air and Marine Operations of U.S. Customs and Border Protection.

(b) UNMANNED AERIAL SYSTEM.—The Secretary of Homeland Security, after coordination with the Administrator of the Federal Aviation Administration, shall ensure that Air and Marine Operations operate unmanned aerial systems on the southern border of the United States for not less than 24 hours per day for 5 days per week.

(c) CONTRACT AIR SUPPORT AUTHORIZATION.—The Commissioner of U.S. Customs and Border Protection may contract for the unfulfilled identified air support mission critical hours, as identified by the Chief of the U.S. Border Patrol.

(d) PRIMARY MISSION.—The Commissioner of U.S. Customs and Border Protection shall ensure that—

(1) the primary missions for Air and Marine Operations are to directly support U.S. Border Patrol activities along the southern border of the United States and Joint Interagency Task Force South operations in the transit zone; and

(2) the Executive Assistant Commissioner of Air and Marine Operations assigns the greatest pri-

ority to support missions established by the Commissioner to carry out the requirements under this Act.

(e) HIGH-DEMAND FLIGHT HOUR REQUIREMENTS.—In accordance with subsection (d), the Commissioner of U.S. Customs and Border Protection shall ensure that U.S. Border Patrol Sector Chiefs—

(1) identify critical flight hour requirements; and

(2) direct Air and Marine Operations to support requests from Sector Chiefs as their primary mission.

(f) SMALL UNMANNED AERIAL VEHICLES.—

(1) IN GENERAL.—The Chief of the U.S. Border Patrol shall be the executive agent for U.S. Customs and Border Protection's use of small unmanned aerial vehicles for the purpose of meeting the U.S. Border Patrol's unmet flight hour operational requirements and to achieve situational awareness and operational control.

(2) COORDINATION.—In carrying out paragraph (1), the Chief of the U.S. Border Patrol shall—

(A) coordinate flight operations with the Administrator of the Federal Aviation Adminis-

1 tration to ensure the safe and efficient oper-
2 ation of the National Airspace System; and
3 (B) coordinate with the Executive Assist-
4 ant Commissioner for Air and Marine Oper-
5 ations of U.S. Customs and Border Protection
6 to ensure the safety of other U.S. Customs and
7 Border Protection aircraft flying in the vicinity
8 of small unmanned aerial vehicles operated by
9 the U.S. Border Patrol.
10 (3) CONFORMING AMENDMENT.—Paragraph (3)
11 of section 411(e) of the Homeland Security Act of
12 2002 (6 U.S.C. 211(e)) is amended—
13 (A) in subparagraph (B), by striking
14 ''and'' after the semicolon at the end;
15 (B) by redesignating subparagraph (C) as
16 subparagraph (D); and
17 (C) by inserting after subparagraph (B)
18 the following new subparagraph:
19 ''(C) carry out the small unmanned aerial
20 vehicle requirements pursuant to section 410(f)
21 of the DHS Authorization Act of 2020; and''.
22 (g) SAVING CLAUSE.—Nothing in this section shall
23 confer, transfer, or delegate to the Secretary, the Commis-
24 sioner, the Executive Assistant Commissioner for Air and
25 Marine Operations of U.S. Customs and Border Protec-

tion, or the Chief of the U.S. Border Patrol any authority of the Secretary of Transportation or the Administrator of the Federal Aviation Administration relating to the use of airspace or aviation safety.

SEC. 412. AMENDMENTS TO U.S. CUSTOMS AND BORDER PROTECTION.

(a) DUTIES.—Subsection (c) of section 411 of the Homeland Security Act of 2002 (6 U.S.C. 211), as amended by this title, is further amended—

(1) in paragraph (20), by striking ''and'' after the semicolon at the end;

(2) by redesignating paragraph (21) as paragraph (23); and

(3) by inserting after paragraph (20) the following new paragraphs:

''(21) administer the U.S. Customs and Border Protection public private partnerships under subtitle G;

''(22) administer preclearance operations under the Preclearance Authorization Act of 2015 (19 U.S.C. 4431 et seq.; enacted as subtitle B of title VIII of the Trade Facilitation and Trade Enforcement Act of 2015; 19 U.S.C. 4301 et seq.); and''.

(b) OFFICE OF FIELD OPERATIONS STAFFING.—Subparagraph (A) of section 411(g)(5) of the Homeland

Security Act of 2002 (6 U.S.C. 211(g)(5)) is amended by inserting before the period at the end the following: ''compared to the number indicated by the current fiscal year work flow staffing model''.

(c) IMPLEMENTATION PLAN.—Subparagraph (B) of section 814(e)(1) of the Preclearance Authorization Act of 2015 (19 U.S.C. 4433(e)(1); enacted as subtitle B of title VIII of the Trade Facilitation and Trade Enforcement Act of 2015; 19 U.S.C. 4301 et seq.) is amended to read as follows:

''(B) a port of entry vacancy rate which compares the number of officers identified in subparagraph (A) with the number of officers at the port at which such officer is currently assigned.''.

(d) DEFINITION.—Subsection (r) of section 411 of the Homeland Security Act of 2002 (6 U.S.C. 211) is amended—

(1) by striking ''this section, the terms'' and inserting the following: ''this section:

''(1) the terms'';

(2) in paragraph (1), as added by subparagraph (A), by striking the period at the end and inserting ''; and''; and

(3) by adding at the end the following new paragraph:

''(2) the term 'unmanned aerial systems' has the meaning given the term 'unmanned aircraft system' in section 44801 of the FAA Modernization and Reform Act of 2018 (Public Law 115–254; 49 U.S.C. 40101 note).''.

SEC. 413. CONTINUOUS SCREENING BY U.S. CUSTOMS AND BORDER PROTECTION.

(a) IN GENERAL.—Subtitle B of title IV of the Homeland Security Act of 2002 (6 U.S.C. 211 et seq.), as amended by this title, is further amended by adding at the end the following new section:

''SEC. 420A. CONTINUOUS SCREENING.

''The Commissioner of U.S. Customs and Border Protection shall, in a risk based manner, continuously screen individuals issued any visa, and individuals who are nationals of a program country pursuant to section 217 of the Immigration and Nationality Act (8 U.S.C. 1187), who are present, or are expected to arrive within 30 days, in the United States, against the appropriate criminal, national security, and terrorism databases maintained by the Federal Government.''.

(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 420, as added by this title, the following new item:

"Sec. 420A. Continuous screening by U.S. Customs and Border Protection.".

SEC. 414. CUSTOMS TRADE PARTNERSHIP AGAINST TERRORISM.

(a) IN GENERAL.—Subtitle B of title II of the Security and Accountability for Every Port Act of 2006 (6 U.S.C. 961 et seq.) is amended to read as follows:

"Subtitle B—Customs Trade Partnership Against Terrorism

"SEC. 211. ESTABLISHMENT OF THE CUSTOMS TRADE PARTNERSHIP AGAINST TERRORISM PROGRAM.

"(a) IN GENERAL.—There is established within U.S. Customs and Border Protection a voluntary government-private sector partnership program to be known as the Customs Trade Partnership Against Terrorism (CTPAT).

"(b) PURPOSE.—The purposes of the CTPAT program are to—

"(1) strengthen and improve the overall security of the international supply chain and United States border security;

"(2) facilitate the movement of secure cargo through the international supply chain;

"(3) ensure compliance with applicable law; and

1 "(4) serve as the Authorized Economic Oper-
2 ator program for the United States.
3 "(c) DIRECTOR.—There shall be at the head of the
4 CTPAT program a Director, who shall report to the Exec-
5 utive Assistant Commissioner of the Office of Field Oper-
6 ations (in this subtitle referred to as the 'Executive Assist-
7 ant Commissioner') of U.S. Customs and Border Protec-
8 tion.
9 "(d) DUTIES.—The Director of the CTPAT program
10 shall—
11 "(1) oversee the activities of the CTPAT pro-
12 gram, including certification of CTPAT participants;
13 "(2) evaluate and make revisions to security
14 criteria pursuant to subsections (c) and (d) of sec-
15 tion 213;
16 "(3) ensure that participants receive a tangible
17 and measurable benefit for participation; and
18 "(4) carry out other duties and powers pre-
19 scribed by the Executive Assistant Commissioner.
20 **"SEC. 212. ELIGIBLE ENTITIES AND NOTICE OF BENEFITS.**
21 "(a) ELIGIBLE ENTITIES.—
22 "(1) IN GENERAL.—Importers, exporters, cus-
23 toms brokers, forwarders, air, sea, and land carriers,
24 contract logistics providers, and other entities in the
25 international supply chain and intermodal transpor-

1 tation system are eligible to apply for participation
2 in the CTPAT program.
3 ''(2) EXPANSION.—The Commissioner may ex-
4 pand the list of entities eligible to apply for CTPAT
5 participation only in accordance with the purpose of
6 the CTPAT program.
7 ''(b) TIERED PARTICIPATION.—
8 ''(1) IN GENERAL.—Applicants specified in sub-
9 section (a) may be eligible to participate as Tier 1
10 or Tier 2 participants.
11 ''(2) IMPORTERS.—Importers may be eligible to
12 participate as Tier 3 participants.
13 ''(3) EXTENSION.—The Commissioner may ex-
14 tend Tier 3 participation to other entity types, if ap-
15 propriate, and to specific Tier 2 CTPAT program
16 participants in accordance with section 217(b).
17 ''(c) NOTICE OF BENEFITS.—
18 ''(1) IN GENERAL.—The Commissioner shall
19 publish, on the U.S. Customs and Border Protection
20 website and through other appropriate online publi-
21 cation, information about benefits available under
22 each tier of the CTPAT program.
23 ''(2) CHANGES.—The Commissioner shall pub-
24 lish, on the U.S. Customs and Border Protection
25 website and through other appropriate online publi-

1 cation, notice of any changes to benefits available
2 under each tier of the CTPAT program not later
3 than 30 days before any such changes take effect.

4 **"SEC. 213. PARTICIPATION ELIGIBILITY.**

5 "(a) IN GENERAL.—The Executive Assistant Com-
6 missioner shall review all documentation submitted by an
7 applicant pursuant to subsection (b)(2), conduct a back-
8 ground investigation of such applicant, and vet such appli-
9 cant.

10 "(b) GENERAL REQUIREMENTS.—To be eligible for
11 participation in the CTPAT program, an entity shall, at
12 a minimum—

13 "(1) have a designated company employee au-
14 thorized to bind such entity who is a direct company
15 employee and will serve as the primary point of con-
16 tact responsible for participation of such entity in
17 the CTPAT program;

18 "(2) at the time of initial application and annu-
19 ally thereafter, including in advance of any recertifi-
20 cation or revalidation, submit an international sup-
21 ply chain security profile, which shall identify how
22 such entity meets the minimum security criteria of
23 the CTPAT program established by the Commis-
24 sioner and how such entity will maintain and en-

1 hance internal policies, procedures, and practices re-
2 lated to international supply chain security; and
3 ''(3) meet any specific requirements for eligible
4 entities, as established by the Commissioner.
5 ''(c) MINIMUM SECURITY CRITERIA.—The Commis-
6 sioner shall establish minimum security criteria for par-
7 ticipants in the CTPAT program, review such minimum
8 security criteria not less than once every two years, and
9 update such minimum security criteria as necessary. Such
10 minimum security criteria shall seek to address security
11 vulnerabilities in the international supply chain.
12 ''(d) ADDITIONAL AND UPDATED CRITERIA.—The
13 Commissioner may establish additional and updated secu-
14 rity criteria for individual CTPAT program participants,
15 categories of CTPAT program participants, or particular
16 entity types to meet in order to address a security vulner-
17 ability in the international supply chain.
18 ''(e) CONSULTATION.—When establishing or updat-
19 ing security criteria in accordance with subsection (c), and
20 when establishing new or updated security criteria in ac-
21 cordance subsection (d), the Commissioner shall consult
22 with CTPAT program participants and other interested
23 parties, and shall—
24 ''(1) conduct a cost benefit analysis of such pro-
25 posed new or updated security criteria, as the case

may be, in consultation with the Commercial Customs Operations Advisory Committee established under section 109 of the Trade Facilitation and Trade Enforcement Act of 2015 (Public Law 114–125; 19 U.S.C. 4316);

''(2) determine operational feasibility and, where appropriate, provide best practices for meeting such new or updated security criteria to CTPAT program participants specific to their entity type;

''(3) conduct a phased implementation of such proposed new or updated security criteria; and

''(4) provide CTPAT program participants and other interested parties a 90-day comment period to review and comment on such proposed new or updated security criteria.

''(f) WAIVER.—The Commissioner may waive the requirements of subsection (e) if the Commissioner determines there is a significant and imminent risk to the national security of the United States and such a waiver is necessary to protect such national security. Not later than 120 days after the issuance of any such waiver, the Commissioner shall announce on the U.S. Customs and Border Protection website and through other appropriate online publication the Commissioner's intent to either withdraw such waiver or maintain such waiver while commencing

efforts to establish new or updated security criteria in accordance with subsection (c) or (d), respectively.

"SEC. 214. BENEFITS FOR CTPAT PROGRAM PARTICIPANTS.

"(a) IN GENERAL.—The Executive Assistant Commissioner shall extend certain benefits to each CTPAT program participant. Minimum benefits for each such participant shall include the following:

"(1) Assignment of a U.S. Customs and Border Protection Supply Chain Security Specialist.

"(2) Access to the CTPAT program's web-based Portal system, training materials, and a mechanism by which to verify other CTPAT program participants' CTPAT status.

"(3) Timely supply chain threat alerts categorized by CTPAT program participant entity type, and an annual and unclassified update made available in such web-based Portal system regarding regional and other relevant threats to the international supply chain.

"(b) ANNUAL ASSESSMENT.—

"(1) IN GENERAL.—The Executive Assistant Commissioner shall conduct, on an annual basis, an assessment of the benefits conferred to CTPAT program participants by tier and entity type. The Executive Assistant Commissioner shall determine a

process to carry out such assessments, including projected milestones and completion dates for addressing data reliability issues and, as necessary, correcting data weaknesses, in order that U.S. Customs and Border Protection can produce accurate and reliable annual assessments that can be compared year-to-year.

"(2) ELEMENTS.—Each annual assessment conducted pursuant to paragraph (1) shall at a minimum include the following:

"(A) The average reduced security exam rate by CTPAT program participant tier and entity type.

"(B) The average reduction in penalties for CTPAT program participants by tier and entity type.

"(C) The average reduction in risk assessment for CTPAT program participants by tier and entity type.

"(3) PUBLIC AVAILABILITY.—The Executive Assistant Commissioner shall make each annual assessment publicly available on the CTPAT portal for at least one year.

"(c) CONSULTATION.—When assessing benefits in accordance with subsection (b), the Executive Assistant

1 Commissioner shall consult with the Commercial Customs
2 Operations Advisory Committee established under section
3 109 of the Trade Facilitation and Trade Enforcement Act
4 of 2015 (Public Law 114–125; 19 U.S.C. 4316) and the
5 National Maritime Security Advisory Committee estab-
6 lished under section 70112 of title 46, United States Code.

7 **"SEC. 215. TIER 1 PARTICIPANTS.**

8 "(a) CERTIFICATION.—The Executive Assistant
9 Commissioner shall certify the security measures and
10 international supply chain security practices of all appli-
11 cants to and participants in the CTPAT program in ac-
12 cordance with section 213(b)(2) and the guidelines re-
13 ferred to in subsection (c) of this section. Certified partici-
14 pants shall be Tier 1 participants.

15 "(b) BENEFITS FOR TIER 1 PARTICIPANTS.—Upon
16 completion of the certification under subsection (a), a
17 CTPAT program participant shall be certified as a Tier
18 1 participant. The Executive Assistant Commissioner shall
19 extend limited benefits to a Tier 1 participant.

20 "(c) CRITERIA.—Not later than 180 days after the
21 date of the enactment of this subtitle, the Commissioner
22 shall update the criteria for certifying a CTPAT program
23 participant's security measures and supply chain security
24 practices under this section. Such criteria shall include a

1 background investigation and review of appropriate docu-
2 mentation, as determined by the Commissioner.

3 ''(d) TIMEFRAME.—To the extent practicable, the
4 Executive Assistant Commissioner shall conclude the Tier
5 1 certification process within 90 days of receipt of a com-
6 pleted application for participation in the CTPAT pro-
7 gram.

8 **''SEC. 216. TIER 2 PARTICIPANTS.**

9 ''(a) VALIDATION.—The Executive Assistant Com-
10 missioner shall validate the security measures and inter-
11 national supply chain security practices of a Tier 1
12 CTPAT program participant in accordance with the
13 guidelines referred to in subsection (c) to validate such
14 participant as a Tier 2 participant. Such validation shall
15 include on-site assessments at appropriate foreign and do-
16 mestic locations utilized by such Tier 1 participant in its
17 international supply chain.

18 ''(b) BENEFITS FOR TIER 2 PARTICIPANTS.—The
19 Executive Assistant Commissioner, shall extend benefits
20 to each CTPAT participant that has been validated as a
21 Tier 2 participant under this section. Such benefits may
22 include the following:

23 ''(1) Reduced scores in U.S. Customs and Bor-
24 der Protection's Automated Targeting System or
25 successor system.

1 ''(2) Reduced number of security examinations
2 by U.S. Customs and Border Protection.
3 ''(3) Penalty mitigation opportunities.
4 ''(4) Priority examinations of cargo.
5 ''(5) Access to the Free and Secure Trade
6 (FAST) Lanes at United States ports of entry.
7 ''(6) Confirmation of CTPAT status to foreign
8 customs administrations that have signed Mutual
9 Recognition Arrangements with U.S. Customs and
10 Border Protection.
11 ''(7) In the case of importers, eligibility to par-
12 ticipate in the Importer Self-Assessment Program
13 (ISA) or successor compliance program.
14 ''(8) In the case of sea carriers, eligibility to
15 participate in the Advance Qualified Unlading Ap-
16 proval (AQUA) Lane process.
17 ''(c) CRITERIA.—Not later than 180 days after the
18 date of the enactment of this subtitle, the Commissioner
19 shall develop a schedule and update the criteria for vali-
20 dating a CTPAT participant's security measures and sup-
21 ply chain security practices under this section.
22 ''(d) TIMEFRAME.—To the extent practicable, the
23 Executive Assistant Commissioner shall complete the Tier
24 2 validation process for a CTPAT program participant

1 under this section within one year after certification of
2 such participant as a Tier 1 participant.

3 **"SEC. 217. TIER 3 PARTICIPANTS.**

4 "(a) IN GENERAL.—The Commissioner shall estab-
5 lish a third tier of CTPAT program participation that of-
6 fers additional benefits to CTPAT program participants
7 that are importers or other entity types, in accordance
8 with section 212(b), that demonstrate a sustained commit-
9 ment to maintaining security measures and international
10 supply chain security practices that exceed the guidelines
11 established for validation as a Tier 2 participant in the
12 CTPAT program under section 216.

13 "(b) BEST PRACTICES.—The Commissioner shall
14 provide a best practices framework to Tier 2 participants
15 interested in Tier 3 status and may designate a Tier 2
16 CTPAT program participant as a Tier 3 participant based
17 on a review of best practices in such participant's inter-
18 national supply chain that reflect a continued approach
19 to enhanced international supply chain security, includ-
20 ing—

21 "(1) compliance with any new or updated cri-
22 teria established by the Commissioner under section
23 213(d) that exceed the guidelines established pursu-
24 ant to section 216 for validating a CTPAT program
25 participant as a Tier 2 participant; and

1 ''(2) any other factors that the Commissioner
2 determines appropriate that are provided in such
3 best practices framework.
4 ''(c) BENEFITS FOR TIER 3 PARTICIPANTS.—The
5 Executive Assistant Commissioner shall extend benefits to
6 each CTPAT program participant that has been validated
7 as a Tier 3 participant under this section, which, in addi-
8 tion to benefits for Tier 2 participation, may include the
9 following:
10 ''(1) Further reduction in the number of exami-
11 nations by U.S. Customs and Border Protection.
12 ''(2) Front of the line inspections and examina-
13 tions.
14 ''(3) Exemption from Stratified Exams.
15 ''(4) Shorter wait times at United States ports
16 of entry.
17 **''SEC. 218. CONSEQUENCES FOR LACK OF COMPLIANCE.**
18 ''(a) IN GENERAL.—If at any time the Executive As-
19 sistant Commissioner determines that a CTPAT program
20 participant's security measures or international supply
21 chain security practices fail to meet applicable require-
22 ments under this subtitle, the Executive Assistant Com-
23 missioner may deny such participant benefits otherwise
24 made available pursuant to this subtitle, either in whole
25 or in part. The Executive Assistant Commissioner shall

1 develop procedures, in consultation with Commercial Cus-
2 toms Operations Advisory Committee established under
3 section 109 of the Trade Facilitation and Trade Enforce-
4 ment Act of 2015 (Public Law 114–125; 19 U.S.C. 4316),
5 that provide appropriate protections to CTPAT program
6 participants, including advance notice and an opportunity
7 for such participants to provide additional information to
8 U.S. Customs and Border Protection regarding any such
9 alleged failure, before any of such benefits are withheld.
10 Such procedures may not limit the ability of the Executive
11 Assistant Commissioner to take actions to protect the na-
12 tional security of the United States.

13 ''(b) FALSE OR MISLEADING INFORMATION; LACK OF
14 COMPLIANCE WITH LAW.—If a CTPAT program partici-
15 pant knowingly provides false or misleading information
16 to the Commissioner, the Executive Assistant Commis-
17 sioner, Director, or any other officers or officials of the
18 United States Government, or if at any time the Executive
19 Assistant Commissioner determines that a CTPAT pro-
20 gram participant has committed a serious violation of
21 Federal law or customs regulations, or if a CTPAT pro-
22 gram participant has committed a criminal violation relat-
23 ing to the economic activity of such participant, the Exec-
24 utive Assistant Commissioner may suspend or remove
25 such participant from the CTPAT program for an appro-

1 priate period of time. The Executive Assistant Commis-
2 sioner, after the completion of the process described in
3 subsection (d), may publish in the Federal Register a list
4 of CTPAT program participants that have been so re-
5 moved from the CTPAT program pursuant to this sub-
6 section.

7 ''(c) NATIONAL SECURITY.—If at any time the Exec-
8 utive Assistant Commissioner determines that a CTPAT
9 program participant poses a significant and imminent risk
10 to the national security of the United States, the Execu-
11 tive Assistant Commissioner may suspend or remove such
12 participant from the CTPAT program for an appropriate
13 period of time. The Executive Assistant Commissioner,
14 after the completion of the process described in subsection
15 (d), may publish in the Federal Register a list of CTPAT
16 program participants that have been so removed from the
17 CTPAT program pursuant to this subsection.

18 ''(d) RIGHT OF APPEAL.—

19 ''(1) IN GENERAL.—The Commissioner shall es-
20 tablish a process for a CTPAT program participant
21 to appeal a decision of the Executive Assistant Com-
22 missioner under subsection (a). Such appeal shall be
23 filed with the Commissioner not later than 90 days
24 after the date of such decision, and the Commis-

sioner shall issue a determination not later than 90 days after such appeal is filed.

"(2) APPEALS OF OTHER DECISIONS.—The Commissioner shall establish a process for a CTPAT program participant to appeal a decision of the Executive Assistant Commissioner under subsections (b) and (c). Such appeal shall be filed with the Commissioner not later than 30 days after the date of such decision, and the Commissioner shall issue a determination not later than 90 days after such appeal is filed.

"SEC. 219. VALIDATIONS BY OTHER DHS COMPONENTS.

"(a) IN GENERAL.—The Commissioner may recognize regulatory inspections of entities conducted by other components of the Department of Homeland Security as sufficient to constitute validation for CTPAT program participation in cases in which any such component's inspection regime is harmonized with validation criteria for the CTPAT program. Such regulatory inspections shall not limit the ability of U.S. Customs and Border Protection to conduct a CTPAT program validation.

"(b) REVALIDATION.—Nothing in this section may limit the Commissioner's ability to require a revalidation by U.S. Customs and Border Protection.

1 ''(c) CERTIFICATION.—Nothing in this section may
2 be construed to authorize certifications of CTPAT appli-
3 cants to be performed by any party other than U.S. Cus-
4 toms and Border Protection.

5 **"SEC. 220. RECERTIFICATION AND REVALIDATION.**

6 ''(a) RECERTIFICATION.—The Commissioner shall
7 implement a recertification process for all CTPAT pro-
8 gram participants. Such process shall occur annually, and
9 shall require—

10 ''(1) a review of the security profile and sup-
11 porting documentation to ensure adherence to the
12 minimum security criteria under section 213; and

13 ''(2) background checks and vetting.

14 ''(b) REVALIDATION.—The Commissioner shall im-
15 plement a revalidation process for all Tier 2 and Tier 3
16 CTPAT program participants. Such process shall re-
17 quire—

18 ''(1) a framework based upon objective, risk-
19 based criteria for identifying participants for peri-
20 odic revalidation at least once every four years after
21 the initial validation of such participants;

22 ''(2) on-site assessments at appropriate foreign
23 and domestic locations utilized by such a participant
24 in its international supply chain; and

1 "(3) an annual plan for revalidation that in-
2 cludes—
3 "(A) performance measures;
4 "(B) an assessment of the personnel need-
5 ed to perform such revalidations; and
6 "(C) the number of participants that will
7 be revalidated during the following year.
8 "(c) REVALIDATION UNDER A MUTUAL RECOGNI-
9 TION ARRANGEMENT.—
10 "(1) IN GENERAL.—Upon request from the
11 Commissioner, all Tier 2 and Tier 3 CTPAT pro-
12 gram participants shall provide any revalidation re-
13 port conducted by a foreign government under a
14 Mutual Recognition Arrangement.
15 "(2) RECOGNITION.—The Commissioner may
16 recognize revalidations of entities conducted by for-
17 eign governments under a Mutual Recognition Ar-
18 rangement as sufficient to constitute a revalidation
19 for CTPAT program participation under subsection
20 (b).
21 "(3) NO LIMITATION.—Nothing in this sub-
22 section may be construed to limit the Commis-
23 sioner's ability to require a revalidation by U.S. Cus-
24 toms and Border Protection.

1 ''(d) DESIGNATED COMPANY EMPLOYEES.—Only
2 designated company employees of a CTPAT program par-
3 ticipant under section 213(b)(1) are authorized to respond
4 to a revalidation report. Third-party entities are not au-
5 thorized to respond to a revalidation report.

6 **''SEC. 221. NONCONTAINERIZED CARGO AND THIRD-PARTY**
7 **LOGISTICS PROVIDERS.**

8 ''The Commissioner shall consider the potential for
9 participation in the CTPAT program by importers of non-
10 containerized cargoes and non-asset-based third-party lo-
11 gistics providers that otherwise meet the requirements
12 under this subtitle.

13 **''SEC. 222. PROGRAM MANAGEMENT.**

14 ''(a) IN GENERAL.—The Commissioner shall estab-
15 lish sufficient internal quality controls and record manage-
16 ment, including recordkeeping (including maintenance of
17 a record management system in accordance with sub-
18 section (b)) and monitoring staff hours, to support the
19 management systems of the CTPAT program. In man-
20 aging the CTPAT program, the Commissioner shall en-
21 sure that the CTPAT program includes the following:

22 ''(1) A five-year plan to identify outcome-based
23 goals and performance measures of the CTPAT pro-
24 gram.

1 ''(2) An annual plan for each fiscal year de-
2 signed to match available resources to the projected
3 workload.
4 ''(3) A standardized work program to be used
5 by agency personnel to carry out the certifications,
6 validations, recertifications, and revalidations of
7 CTPAT program participants.
8 ''(4) In accordance with subsection (e), a stand-
9 ardized process for the Executive Assistant Commis-
10 sioner to receive reports of suspicious activity, in-
11 cluding reports regarding potentially compromised
12 cargo or other national security concerns.
13 ''(b) DOCUMENTATION OF REVIEWS.—
14 ''(1) IN GENERAL.—The Commissioner shall
15 maintain a record management system to document
16 determinations on the reviews of each CTPAT pro-
17 gram participant, including certifications, valida-
18 tions, recertifications, and revalidations.
19 ''(2) STANDARDIZED PROCEDURES.—To ensure
20 accuracy and consistency within the record manage-
21 ment system required under this subsection, the
22 Commissioner shall develop, disseminate, and re-
23 quire utilization of standardized procedures for
24 agency personnel carrying out certifications, valida-
25 tions, recertifications, and revalidations to report

and track information regarding the status of each CTPAT program participant.

"(c) CONFIDENTIAL INFORMATION SAFEGUARDS.—In consultation with the Commercial Customs Operations Advisory Committee established under section 109 of the Trade Facilitation and Trade Enforcement Act of 2015 (Public Law 114–125; 19 U.S.C. 4316), the Commissioner shall develop and implement procedures to ensure the protection of confidential data collected, stored, or shared with government agencies or as part of the application, certification, validation, recertification, and revalidation processes.

"(d) RESOURCE MANAGEMENT STAFFING PLAN.—The Commissioner shall—

"(1) develop a staffing plan to recruit and train staff (including a formalized training program) to meet the objectives identified in the five-year strategic plan under subsection (a)(1); and

"(2) provide cross-training in post incident trade resumption for the CTPAT Director and other relevant personnel who administer the CTPAT program.

"(e) ENGAGEMENT.—In carrying out the standardized process required under subsection (a)(4), the Commissioner shall engage with and provide guidance to

1 CTPAT program participants and other appropriate
2 stakeholders on submitting reports described in such sub-
3 section.

4 ''(f) REPORT TO CONGRESS.—In connection with the
5 President's annual budget submission for the Department
6 of Homeland Security, the Commissioner shall report to
7 the appropriate congressional committees on the progress
8 made by the Commissioner to certify, validate, recertify,
9 and revalidate CTPAT program participants. Each such
10 report shall be due on the same date that the President's
11 budget is submitted to Congress.''.

12 (b) SAVING CLAUSE.—

13 (1) IN GENERAL.—The amendments made by
14 this Act shall take effect and apply beginning on the
15 date that is 90 days after the date of the enactment
16 of this Act with respect to applicants for participa-
17 tion in the CTPAT program.

18 (2) EXCEPTION.—Paragraph (1) shall not
19 apply in case of CTPAT program participants who
20 are such participants as of the date specified in such
21 paragraph. Such participants shall be subject to the
22 amendments made by this Act upon revalidation of
23 such participants to participate in such program.
24 Until such time, such participants shall be subject to
25 the requirements of the CTPAT program as in exist-

ence on the day before the date of the enactment of this Act.

(c) TECHNICAL AND CONFORMING AMENDMENTS.—The Security and Accountability for Every Port Act of 2006 is amended—

(1) in paragraph (4) of section 2 (6 U.S.C. 901), by striking ''Commissioner responsible for the United States Customs and Border Protection'' and inserting ''Commissioner of U.S. Customs and Border Protection''; and

(2) in paragraph (2) of section 202(c) (6 U.S.C. 942(c)), by striking ''C–TPAT'' and inserting ''CTPAT''.

(d) CLERICAL AMENDMENTS.—The table of contents in section 1(b) of the Security and Accountability for Every Port Act of 2006 is amended by striking the items relating to subtitle B of title II and inserting the following new items:

''Subtitle B—Customs Trade Partnership Against Terrorism

''Sec. 211. Establishment of the Customs Trade Partnership Against Terrorism program.
''Sec. 212. Eligible entities and notice of benefits.
''Sec. 213. Participation eligibility.
''Sec. 214. Benefits for CTPAT program participants.
''Sec. 215. Tier 1 participants.
''Sec. 216. Tier 2 participants.
''Sec. 217. Tier 3 participants.
''Sec. 218. Consequences for lack of compliance.
''Sec. 219. Validations by other DHS components.
''Sec. 220. Recertification and revalidation.
''Sec. 221. Noncontainerized cargo and third-party logistics providers.
''Sec. 222. Program management.''.

SEC. 415. STRATEGY TO ENSURE DETECTION OF ALL OPIOID PURITY LEVELS AT PORTS OF ENTRY.

(a) IN GENERAL.—Not later than 180 days after the date of the enactment of this section, the Commissioner of U.S. Customs and Border Protection (CBP) shall—

(1) implement a strategy to ensure deployed chemical screening devices are able to identify, in an operational environment, narcotics at purity levels less than or equal to 10 percent, or provide ports of entry with an alternate method for identifying narcotics at lower purity levels; and

(2) require testing of any new chemical screening devices to understand the abilities and limitations of such devices relating to identifying narcotics at various purity levels before CBP commits to the acquisition of such devices.

(b) PLAN TO ENSURE OPIOID DETECTION EQUIPMENT RESILIENCY.—Not later than 180 days after the date of the enactment of this section, the Secretary of Homeland Security shall implement a plan for the long-term development of a centralized spectral database for chemical screening devices. Such plan shall address the following:

(1) How newly identified spectra will be collected, stored, and distributed to such devices in

their operational environment, including at ports of entry.

(2) Identification of parties responsible for updates and maintenance of such database.

SEC. 416. AUTHORIZATION OF THE IMMIGRATION ADVISORY PROGRAM.

(a) IN GENERAL.—Subtitle B of title IV of the Homeland Security Act of 2002 (6 U.S.C. 211 et seq.), as amended by this title, is further amended by adding at the end the following new section:

"SEC. 420B. IMMIGRATION ADVISORY PROGRAM.

''(a) IN GENERAL.—There is authorized within U.S. Customs and Border Protection an immigration advisory program (in this section referred to as the 'program') for United States Customs and Border Protection officers, pursuant to an agreement with a host country, to assist air carriers and security employees at foreign airports with review of traveler information during the processing of flights bound for the United States.

''(b) ACTIVITIES.—In carrying out the program, U.S. Customs and Border Protection officers may—

''(1) be present during processing of flights bound for the United States;

1 ''(2) assist air carriers and security employees
2 with document examination and traveler security as-
3 sessments;
4 ''(3) provide relevant training to air carriers,
5 security employees, and host-country authorities;
6 ''(4) analyze electronic passenger information
7 and passenger reservation data to identify potential
8 threats;
9 ''(5) engage air carriers and travelers to con-
10 firm potential terrorist watchlist matches;
11 ''(6) make recommendations to air carriers to
12 deny potentially inadmissible passengers boarding
13 flights bound for the United States; and
14 ''(7) conduct other activities to secure flights
15 bound for the United States, as directed by the
16 Commissioner of United States Customs and Border
17 Protection.
18 ''(c) NOTIFICATION TO CONGRESS.—Not later than
19 60 days before an agreement with the government of a
20 host country pursuant to the program described in this
21 section enters into force, the Commissioner of U.S. Cus-
22 toms and Border Protection shall provide the Committee
23 on Homeland Security of the House of Representatives
24 and the Committee on Homeland Security and Govern-
25 mental Affairs of the Senate with—

"(1) a copy of such agreement, which shall include—

"(A) the identification of the host country with which United States Customs and Border Protection intends to enter into such agreement;

"(B) the location at which activities described in subsection (b) will be conducted pursuant to such agreement; and

"(C) the terms and conditions for United States Customs and Border Protection personnel operating at such location;

"(2) country-specific information on the anticipated homeland security benefits associated with such agreement;

"(3) an assessment of the impacts such agreement will have on United States Customs and Border Protection domestic port of entry staffing;

"(4) information on the anticipated costs over the 5 fiscal years after such agreement enters into force associated with carrying out such agreement;

"(5) details on information sharing mechanisms to ensure that United States Customs and Border Protection has current information to prevent terrorist and criminal travel; and

"(6) other factors that the Commissioner determines necessary for Congress to comprehensively assess the appropriateness of carrying out the program.

"(d) AMENDMENT OF EXISTING AGREEMENTS.—Not later than 30 days before a substantially amended program agreement with the government of a host country in effect as of the date of the enactment of this section enters into force, the Commissioner of U.S. Customs and Border Protection 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—

"(1) a copy of such agreement, as amended; and

"(2) the justification for such amendment.

"(e) DEFINITIONS.—In this section, the terms 'air carrier' and 'foreign air carrier' have the meanings given such terms in section 40102 of title 49, United States Code.".

(b) CONFORMING AMENDMENT.—Subsection (c) of section 411 of the Homeland Security Act of 2002 (6 U.S.C. 211), as amended by this title, is further amended—

(1) in paragraph (22), by striking ''and'' after the semicolon at the end;

(2) by redesignating paragraph (23) as paragraph (24); and

(3) by inserting after paragraph (22) the following new paragraph:

''(23) carry out section 420B, relating to the immigration advisory program; and''.

(c) 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 420A, as added by this title, the following new item:

''Sec.420B. Immigration advisory program.''.

SEC. 417. BORDER SECURITY TECHNOLOGY ACCOUNTABILITY.

(a) IN GENERAL.—Subtitle C of title IV of the Homeland Security Act of 2002 (6 U.S.C. 231 et seq.) is amended by adding at the end the following new section:

''SEC. 437. BORDER SECURITY TECHNOLOGY PROGRAM MANAGEMENT.

''(a) PLANNING DOCUMENTATION.—For each border security technology acquisition program of the Department that is determined to be a major acquisition program, the Secretary shall—

1 ''(1) ensure that each such program has a writ-
2 ten acquisition program baseline approved by the
3 relevant acquisition decision authority;
4 ''(2) document that each such program is meet-
5 ing cost, schedule, and performance thresholds as
6 specified in such baseline, in compliance with rel-
7 evant departmental acquisition policies and the Fed-
8 eral Acquisition Regulation; and
9 ''(3) have a plan for meeting program imple-
10 mentation objectives by managing contractor per-
11 formance.
12 ''(b) ADHERENCE TO STANDARDS.—The Secretary,
13 acting through the Under Secretary for Management and
14 the Commissioner of U.S. Customs and Border Protection,
15 shall ensure border security technology acquisition pro-
16 gram managers who are responsible for carrying out this
17 section adhere to relevant internal control standards iden-
18 tified by the Comptroller General of the United States.
19 The Commissioner shall provide information, as needed,
20 to assist the Under Secretary in monitoring management
21 of border security technology acquisition programs under
22 this section.
23 ''(c) PLAN.—The Secretary, acting through the
24 Under Secretary for Management, in coordination with
25 the Under Secretary for Science and Technology and the

1 Commissioner of U.S. Customs and Border Protection,
2 shall submit to the appropriate congressional committees
3 a plan for testing, evaluating, and using independent
4 verification and validation resources for border security
5 technology. Under the plan, new border security tech-
6 nologies shall be evaluated through a series of assess-
7 ments, processes, and audits to ensure compliance with
8 relevant departmental acquisition policies and the Federal
9 Acquisition Regulation, as well as the effectiveness of tax-
10 payer dollars.

11 ''(d) MAJOR ACQUISITION PROGRAM DEFINED.—In
12 this section, the term 'major acquisition program' means
13 a Department acquisition program that is estimated by
14 the Secretary to require an eventual total expenditure of
15 at least $300,000,000 (based on fiscal year 2021 constant
16 dollars) over its life cycle cost.''.

17 (e) CLERICAL AMENDMENT.—The table of contents
18 of the Homeland Security Act of 2002 is amended by
19 striking the items relating to sections 435 and 436 and
20 inserting after the item relating to section 434 the fol-
21 lowing new items:

''Sec. 435. Maritime operations coordination plan.
''Sec. 436. Maritime security capabilities assessments.
''Sec. 437. Border security technology program management.''.

SEC. 418. ESTABLISHMENT OF U.S. IMMIGRATION AND CUSTOMS ENFORCEMENT.

(a) IN GENERAL.—Section 442 of the Homeland Security Act of 2002 (6 U.S.C. 252) is amended to read as follows:

"SEC. 442. U.S. IMMIGRATION AND CUSTOMS ENFORCEMENT.

"(a) ESTABLISHMENT.—There is established within the Department an agency to be known as U.S. Immigration and Customs Enforcement.

"(b) DIRECTOR OF U.S. IMMIGRATION AND CUSTOMS ENFORCEMENT.—There shall be at the head of U.S. Immigration and Customs Enforcement a Director of U.S. Immigration and Customs Enforcement (in this section referred to as the 'Director').

"(c) DUTIES AND QUALIFICATIONS.—The Director shall—

"(1) have a minimum of five years—

"(A) professional experience in law enforcement, which may include law enforcement as it relates to the immigration laws, as defined in paragraph (17) of section 101(a) of the Immigration and Nationality Act (8 U.S.C. 1101(a)(17)) or the customs and trade laws of the United States, as defined in section 2 of the

Trade Facilitation and Trade Enforcement Act of 2015 (19 U.S.C. 4301); and

"(B) management experience;

"(2) in coordination with U.S. Customs and Border Protection and United States Citizenship and Immigration Services, enforce and administer immigration laws, as defined in paragraph (17) of section 101(a) of the Immigration and Nationality Act (8 U.S.C. 1101(a)), including the identification, arrest, detention, and removal of aliens who may be inadmissible to, or deportable from, the United States;

"(3) have the authority to investigate and, where appropriate, refer for prosecution, any criminal or civil violation of Federal law relating to or involving—

"(A) border control and security, including the prevention of the entry or residence of terrorists, criminals, and human rights violators;

"(B) the customs and trade laws of the United States, as defined in section 2 of the Trade Facilitation and Trade Enforcement Act of 2015 (19 U.S.C. 4301);

"(C) fraud, false statements, or other violations on the import or export of merchandise,

including the illicit possession, movement of, or trade in goods, services, property, arms, instruments of terrorism, items controlled or prohibited from export, goods made with forced or indentured labor, intellectual property, or currency or other monetary instruments;

''(D) bulk cash smuggling or other financial crimes with a cross-border or international nexus;

''(E) the immigration laws, as defined in paragraph (17) of section 101(a) of the Immigration and Nationality Act (8 U.S.C. 1101(a));

''(F) transnational organized crime;

''(G) chapter 40 or 44 of title 18, United States Code, or other violation relating to explosives, firearms, other destructive devices involving an alien;

''(H) severe forms of trafficking in persons, as defined in section 103 of the Victims of Trafficking and Violence Protection Act of 2000 (22 U.S.C. 7102);

''(I) the production, procurement, counterfeiting, alteration, or use of fraudulent immigration documents or fraudulently obtaining immigration benefits;

"(J) unlawful use of personal information, when such use relates to or affects border security, terrorism, customs, immigration, naturalization, trade, or transportation security;

"(K) computer crimes, pursuant to section 1030(d) of title 18, United States Code, in cooperation, where required by law, with the United States Secret Service and the Federal Bureau of Investigation;

"(L) drug laws, as specified in the Controlled Substances Act and the Controlled Substances Import and Export Act in the context of cross-border criminal activity;

"(M) child exploitation, child pornography, or traveling child sex offenders pursuant to section 890A(b)(2)(A) of the Homeland Security Act of 2002 (6 U.S.C. 473(b)(2)(A)); and

"(N) cyber-enabled crimes pursuant to section 890A(d)(2)(B) of the Homeland Security Act of 2002 (6 U.S.C. 473(d)(2)(B));

"(4) administer the National Intellectual Property Rights Coordination Center established in section 305 of the Trade Facilitation and Trade Enforcement Act of 2015 (Public Law 114–125; 19 U.S.C. 4344);

"(5) jointly with the Commissioner of U.S. Customs and Border Protection, develop and submit the joint strategic plan required under section 105 of the Trade Facilitation and Trade Enforcement Act of 2015 (Public Law 114–125; 19 U.S.C. 4314);

"(6) coordinate, as otherwise permitted by law, with Federal, State, local, tribal, and foreign agencies in carrying out the duties set forth in paragraphs (2) and (3);

"(7) in coordination with the Office of International Affairs of the Department and the Department of State, establish staff liaison offices and vetted units in foreign countries to support law enforcement activities that require international cooperation, including investigations and repatriation efforts;

"(8) assign employees of the Department to diplomatic and consular posts, in coordination with the Secretary, pursuant to section 428(e);

"(9) authorize danger pay allowance for employees of the Department pursuant to section 5928 of title 5, United States Code, with the approval of the Secretary of State;

"(10) provide technical assistance and training to trusted and vetted law enforcement and customs

1 authorities of foreign countries to enhance the abil-
2 ity of such authorities to enforce immigration and
3 customs laws;
4 ''(11) establish, maintain, and administer ap-
5 propriate law enforcement centers, including the
6 Human Rights Violators and War Crimes Center
7 and other interagency centers, in accordance with
8 applicable law, or as prescribed by the Secretary or
9 in furtherance of the Director's assigned duties;
10 ''(12) administer the Border Enforcement Secu-
11 rity Task Force established under section 432;
12 ''(13) operate the Cyber Crimes Center estab-
13 lished in section 890A;
14 ''(14) in carrying out paragraph (3), administer
15 internal conspiracy investigations at United States
16 ports of entry; and
17 ''(15) carry out other duties and powers pre-
18 scribed by law or delegated by the Secretary.
19 ''(d) GENERAL ENFORCEMENT POWERS.—The Di-
20 rector may authorize agents and officers of U.S. Immigra-
21 tion and Customs Enforcement to—
22 ''(1) carry out the duties and responsibilities
23 authorized under section 287 of the Immigration
24 and Nationality Act (8 U.S.C. 1357) and section
25 589 of the Tariff Act of 1930 (19 U.S.C. 1589a);

1 ''(2) seize any property, whether real or per-
2 sonal, that is involved in any violation or attempted
3 violation, or which constitutes proceeds traceable to
4 a violation, of those provisions of law which U.S. Im-
5 migration and Customs Enforcement is authorized
6 to enforce;
7 ''(3) offer and pay rewards for services and in-
8 formation regarding the apprehension of persons in-
9 volved in, or the seizure and forfeiture of property
10 associated with, the violation or attempted violation
11 of those provisions of law which U.S. Immigration
12 and Customs Enforcement is authorized to enforce;
13 ''(4) issue detainers for purposes of immigra-
14 tion enforcement pursuant to sections 236, 241, and
15 287 of the Immigration and Nationality Act (8
16 U.S.C. 1226, 1231, and 1357); and
17 ''(5) conduct undercover investigative oper-
18 ations pursuant to section 294 of the Immigration
19 and Nationality Act (8 U.S.C. 1363a), and section
20 3131 of the Customs Enforcement Act of 1986 (19
21 U.S.C. 2081; enacted as part of the Anti-Drug
22 Abuse Act of 1986).
23 ''(e) DEPUTY DIRECTOR.—There shall be in U.S. Im-
24 migration and Customs Enforcement a Deputy Director

1 who shall assist the Director in the management of U.S.
2 Immigration and Customs Enforcement.
3 "(f) OFFICE OF HOMELAND SECURITY INVESTIGA-
4 TIONS.—
5 "(1) IN GENERAL.—There is established in
6 U.S. Immigration and Customs Enforcement the Of-
7 fice of Homeland Security Investigations.
8 "(2) EXECUTIVE ASSOCIATE DIRECTOR.—There
9 shall be at the head of the Office of Homeland Secu-
10 rity Investigations an Executive Associate Director,
11 who shall report to the Director.
12 "(3) DUTIES.—The Office of Homeland Secu-
13 rity Investigations shall—
14 "(A) serve as the law enforcement office of
15 U.S. Immigration and Customs Enforcement
16 with primary responsibility to conduct investiga-
17 tions of terrorist organizations and other crimi-
18 nal organizations that threaten the homeland or
19 border security;
20 "(B) serve as the law enforcement office of
21 U.S. Immigration and Customs Enforcement
22 with primary responsibility to conduct investiga-
23 tions of, and, where appropriate, refer for pros-
24 ecution, any criminal or civil violations of Fed-
25 eral law, including—

1 ''(i) financial crimes;
2 ''(ii) money laundering and bulk cash
3 smuggling;
4 ''(iii) commercial fraud and intellec-
5 tual property theft;
6 ''(iv) cyber-enabled crimes pursuant to
7 section 890A(d)(2)(B) of the Homeland
8 Security Act of 2002 (6 U.S.C.
9 473(d)(2)(B));
10 ''(v) human smuggling, human traf-
11 ficking, and human rights violations;
12 ''(vi) narcotics and weapons smug-
13 gling and trafficking;
14 ''(vii) transnational gang activity;
15 ''(viii) export violations;
16 ''(ix) international art and antiquity
17 theft;
18 ''(x) identity and benefit fraud;
19 ''(xi) unlawful employment of unau-
20 thorized aliens;
21 ''(xii) child exploitation, child pornog-
22 raphy, and traveling child sex offenders
23 pursuant to section 890A(b)(2)(A) of the
24 Homeland Security Act of 2002 (6 U.S.C.
25 473(b)(2)(A));

1 ''(xiii) computer crimes pursuant to
2 section 1030(d) of title 18, United States
3 Code, in cooperation, where required by
4 law, with the United States Secret Service
5 and the Federal Bureau of Investigation;
6 and
7 ''(xiv) any other criminal or civil viola-
8 tion prescribed by law or delegated by the
9 Director;
10 ''(C) administer the program to collect in-
11 formation relating to nonimmigrant foreign stu-
12 dents and exchange visitor program partici-
13 pants described in section 641 of the Illegal Im-
14 migration Reform and Immigrant Responsibility
15 Act of 1996 (8 U.S.C. 1372), including the
16 Student and Exchange Visitor Information Sys-
17 tem established under such section, and use
18 such information to carry out the enforcement
19 functions of U.S. Immigration and Customs
20 Enforcement; and
21 ''(D) carry out other duties and powers
22 prescribed by the Director.
23 ''(g) OFFICE OF ENFORCEMENT AND REMOVAL OP-
24 ERATIONS.—

1 "(1) IN GENERAL.—There is established in
2 U.S. Immigration and Customs Enforcement the Of-
3 fice of Enforcement and Removal Operations.
4 "(2) EXECUTIVE ASSOCIATE DIRECTOR.—There
5 shall be at the head of the Office of Enforcement
6 and Removal Operations an Executive Associate Di-
7 rector, who shall report to the Director.
8 "(3) DUTIES.—The Office of Enforcement and
9 Removal Operations shall—
10 "(A) serve as the law enforcement office of
11 U.S. Immigration and Customs Enforcement
12 with primary responsibility to enforce the civil
13 immigration and nationality laws of the United
14 States, except to the extent that any other
15 agency of the Federal Government has the re-
16 sponsibility or authority for so doing;
17 "(B) identify, locate, detain, and arrest
18 aliens in custodial settings or at-large who may
19 be subject to removal from the United States;
20 "(C) have custody over (and the authority
21 to release) aliens detained for potential exclu-
22 sion, deportation, or removal from the United
23 States, manage the administrative immigration
24 detention operations of U.S. Immigration and
25 Customs Enforcement, and provide necessary

and appropriate medical care and dental and mental health services to detained aliens in the custody of the agency;

"(D) plan, coordinate, and manage the execution of exclusion, deportation, and removal orders issued to aliens;

"(E) investigate and refer for prosecution any civil or criminal violation of the immigration laws or any offense described in section 287(a)(5) of the Immigration and Nationality Act (8 U.S.C. 1357(a)(5)); and

"(F) carry out other duties and powers prescribed by the Director.

"(h) OFFICE OF THE PRINCIPAL LEGAL ADVISOR.—

"(1) IN GENERAL.—There is established in U.S. Immigration and Customs Enforcement the Office of the Principal Legal Advisor.

"(2) PRINCIPAL LEGAL ADVISOR.—There shall be at the head of the Office the Principal Legal Advisor a Principal Legal Advisor.

"(3) DUTIES.—The Office of the Principal Legal Advisor shall—

"(A) provide specialized legal advice to the Director;

1 "(B) represent U.S. Immigration and Cus-
2 toms Enforcement in all exclusion, deportation,
3 and removal proceedings before the Executive
4 Office for Immigration Review; and
5 "(C) carry out other duties and powers
6 prescribed by the Director.
7 "(i) OFFICE OF PROFESSIONAL RESPONSIBILITY.—
8 "(1) IN GENERAL.—There is established in
9 U.S. Immigration and Customs Enforcement the Of-
10 fice of Professional Responsibility.
11 "(2) ASSOCIATE DIRECTOR.—There shall be at
12 the head of the Office of Professional Responsibility
13 an Associate Director, who shall report to the Direc-
14 tor.
15 "(3) DUTIES.—The Office of Professional Re-
16 sponsibility shall—
17 "(A) investigate allegations of criminal,
18 civil, or administrative misconduct involving any
19 employee, officer, or contractor of U.S. Immi-
20 gration and Customs Enforcement;
21 "(B) inspect and review U.S. Immigration
22 and Customs Enforcement's offices, operations,
23 and processes, including detention facilities op-
24 erated or used by U.S. Immigration and Cus-
25 toms Enforcement, and provide an independent

review of U.S. Immigration and Custom Enforcement's organizational health, effectiveness, and efficiency of mission;

"(C) provide and manage the security programs and operations for U.S. Immigration and Customs Enforcement; and

"(D) carry out other duties and powers prescribed by the Director.

"(j) OFFICE OF MANAGEMENT AND ADMINISTRATION.—

"(1) IN GENERAL.—There is established in U.S. Immigration and Customs Enforcement the Office of Management and Administration.

"(2) EXECUTIVE ASSOCIATE DIRECTOR.—There shall be at the head of the Office of Management and Administration an Executive Associate Director, who shall report to the Director.

"(3) DUTIES.—The Office of Management and Administration shall—

"(A) oversee and execute the agency's administrative and management support functions to ensure compliance with all laws, regulations and policies, sound resource and asset management, internal controls, and in furtherance of ICE mission effectiveness;

1 ''(B) oversee the delivery of ICE's budget
2 justifications, manage budget distributions, and
3 oversee the execution of ICE's budget through
4 financial policies, standards, and systems for
5 ICE's programs, projects, and activities;
6 ''(C) deliver human capital programs on
7 behalf of the agency;
8 ''(D) establish acquisition strategies, per-
9 form oversight for all investments, ensure pro-
10 gram accountability, and perform oversight and
11 execution of all contracting activities;
12 ''(E) manage ICE's facilities portfolio en-
13 suring infrastructure is effectively planned, ac-
14 quired, and maintained;
15 ''(F) develop and maintain an integrated
16 information technology infrastructure;
17 ''(G) ensure the implementation of strong
18 privacy protections, records management, data
19 governance practices, and timely responses to
20 Freedom of Information Act requests;
21 ''(H) develop and execute leadership and
22 career development programs to meet ICE
23 training needs; and
24 ''(I) carry out other duties and authorities
25 prescribed by the Director.

1 ''(k) OTHER AUTHORITIES.—
2 ''(1) IN GENERAL.—The Secretary may estab-
3 lish such other Executive Associate Directors, As-
4 sistant Directors, or other similar officers or offi-
5 cials, or other offices or positions as the Secretary
6 determines necessary to carry out the missions, du-
7 ties, functions, and authorities of U.S. Immigration
8 and Customs Enforcement.
9 ''(2) NOTIFICATION.—If the Secretary exercises
10 the authority provided pursuant to paragraph (1),
11 the Secretary shall notify the Committee on Home-
12 land Security and the Committee on the Judiciary of
13 the House of Representatives and the Committee on
14 Homeland Security and Governmental Affairs and
15 the Committee on the Judiciary of the Senate not
16 later than 30 days before exercising such authority.
17 ''(l) OTHER FEDERAL AGENCIES.—Nothing in this
18 section may be construed as affecting or limiting in any
19 manner the authority, as in existence on the day before
20 the date of the enactment of this section, of any other
21 Federal agency or other component of the Department.''.
22 (b) SPECIAL RULES.—
23 (1) TREATMENT.—Section 442 of the Home-
24 land Security Act of 2002, as amended by subsection
25 (a) of this section, shall be treated as if included in

such Act as of the date of the enactment of such Act. In addition to the functions, missions, duties, and authorities specified in such amended section 442, U.S. Immigration and Customs Enforcement shall continue to perform and carry out the functions, missions, duties, and authorities under section 442 of such Act as in existence on the day before such date of enactment (notwithstanding the treatment described in this paragraph).

(2) RULES OF CONSTRUCTION.—

(A) RULES AND REGULATIONS.—Notwithstanding the treatment described in paragraph (1), nothing in this Act may be construed as affecting in any manner any rule or regulation issued or promulgated pursuant to any provision of law, including section 442 of the Homeland Security Act of 2002, as in existence on the day before the date of the enactment of this Act, and any such rule or regulation shall continue to have full force and effect on and after such date.

(B) OTHER ACTIONS.—Notwithstanding the treatment described in paragraph (1), nothing in this Act may be construed as affecting in any manner any action, determination, policy,

or decision pursuant to section 442 of the Homeland Security Act of 2002 as in existence on the day before the date of the enactment of this Act, and any such action, determination, policy, or decision shall continue to have full force and effect on and after such date.

(c) CONTINUATION IN OFFICE.—

(1) DIRECTOR.—The individual serving as the Director of U.S. Immigration and Customs Enforcement on the day before the date of the enactment of this Act (notwithstanding the treatment described in subsection (b)(1)) may serve as the Director of U.S. Immigration and Customs Enforcement in accordance with section 442 of the Homeland Security Act of 2002, as amended by subsection (a), until the earlier of—

(A) the date on which such individual is no longer eligible to serve as Director; or

(B) the date on which a person nominated by the President to be the Director is confirmed by the Senate in accordance with such section 441.

(2) OTHER POSITIONS.—The individuals serving as the Deputy Director, Executive Associate Directors, Deputy Executive Associate Directors, or

similar officers or officials of U.S. Immigration and Customs Enforcement under section 442 of the Homeland Security Act of 2002 on the day before the date of the enactment of this Act (notwithstanding the treatment described in subsection (b)(1)) may serve as the appropriate Deputy Director, Executive Associate Directors, Deputy Executive Associate Directors, Associate Directors, Deputy Associate Directors, Assistant Directors, and other officers and officials under section 442 of such Act, as amended by subsection (a), unless the individual serving as the Director of U.S. Immigration and Customs Enforcement determines that another individual should hold such position.

(d) TRANSPORTATION.—Paragraph (6) of section 1344(b) of title 31, United States Code, is amended by inserting ", the Director of U.S. Immigration and Customs Enforcement, the Commissioner of Customs and Border Protection," before "the Administrator of the Drug Enforcement Administration,".

(e) CONFORMING AMENDMENTS.—

(1) TITLE 5.—Section 5314 of title 5, United States Code, is amended by inserting after "Director of the Bureau of Citizenship and Immigration Serv-

ices.'' the following new item: ''Director of U.S. Immigration and Customs Enforcement.''.

(2) TITLE 18.—Subsection (d) of section 1030 of title 18, United States Code, is amended—

(A) in paragraph (1), by inserting ''and U.S. Immigration and Customs Enforcement'' after ''United States Secret Service'';

(B) in paragraph (2), by inserting, '', in collaboration with U.S. Immigration and Customs Enforcement'' after ''Federal Bureau of Investigation''; and

(C) in paragraph (3), by striking ''Secretary of the Treasury'' and inserting ''Secretary of Homeland Security''.

(3) TRADE FACILITATION AND TRADE ENFORCEMENT ACT OF 2015.—Paragraph (2) of section 802(d) of the Trade Facilitation and Trade Enforcement Act of 2015 (Public Law 114–125) is amended by inserting before the period at the end the following: ''or the Director of U.S. Immigration and Customs Enforcement, as determined by the Secretary of Homeland Security''.

(4) HOMELAND SECURITY ACT OF 2002.—Title IV of the Homeland Security Act of 2002 is amended—

(A) in subtitle C—

(i) in subsection (e) of section 428 (6 U.S.C. 236), by adding at the end the following new paragraph:

"(9) DELEGATED AUTHORITY.—For purposes of this subsection, the Secretary shall act through the Director of U.S. Immigration and Customs Enforcement."; and

(ii) in section 432 (6 U.S.C. 240)—

(I) by redesignating subsection (e) as subsection (f); and

(II) by inserting after subsection (d) the following new subsection:

"(e) ADMINISTRATION.—The Director of U.S. Immigration and Customs Enforcement shall administer BEST units established under this section.";

(B) in subtitle D—

(i) by amending the subtitle heading to read as follows: "**U.S. Immigration and Customs Enforcement**"; and

(ii) by repealing sections 445 and 446 (6 U.S.C. 255 and 256);

(C) in subtitle E—

(i) in subsection (a)(2)(C) of section 451 (6 U.S.C. 271), by striking "at the

same level as the Assistant Secretary of the Bureau of Border Security'' and inserting ''in accordance with section 5314 of title 5, United States Code'';

(ii) in subsection (c) of section 459 (6 U.S.C. 276), by striking ''Assistant Secretary of the Bureau of Border Security'' and inserting ''Director of U.S. Immigration and Customs Enforcement''; and

(iii) in subsection (b)(2)(A) of section 462 (6 U.S.C. 279), in the matter preceding clause (i), by striking ''Assistant Secretary of the Bureau of Border Security'' and inserting ''Director of U.S. Immigration and Customs Enforcement''; and

(D) in subtitle F, in subsection (a)(2)(B) of section 472 (6 U.S.C. 292), by striking ''Bureau of Border Security'' and inserting ''U.S. Immigration and Customs Enforcement''.

(f) CLERICAL AMENDMENTS.—The table of contents in section 1(b) of such Act is amended—

(1) by striking the item relating to subtitle D of title IV and inserting the following new item:

"Subtitle D—U.S. Immigration and Customs Enforcement".."; and

(2) by striking the items relating sections 445 and 446.

SEC. 419. BIOMETRIC IDENTIFICATION TRANSNATIONAL MIGRATION ALERT PROGRAM.

(a) IN GENERAL.—Subtitle D of title IV of the Homeland Security Act of 2002 (6 U.S.C. 251 et seq.), as amended by this title, is further amended by adding at the end the following new section:

"SEC. 445. BIOMETRIC IDENTIFICATION TRANSNATIONAL MIGRATION ALERT PROGRAM.

''(a) ESTABLISHMENT.—There is established in the Department a program to be known as the 'Biometric Identification Transnational Migration Alert Program' (referred to in this section as 'BITMAP') to address and reduce national security, border security, and terrorist threats before such threats reach the international border of the United States.

''(b) DUTIES.—In carrying out BITMAP operations, the Secretary, acting through the Director of U.S. Immigration and Customs Enforcement, shall—

''(1) coordinate, in consultation with the Secretary of State, appropriate representatives of foreign governments, and the heads of other Federal

1 agencies, as appropriate, to facilitate the voluntary
2 sharing of biometric and biographic information col-
3 lected from foreign nationals for the purpose of iden-
4 tifying and screening such nationals to identify indi-
5 viduals who may pose a terrorist threat or a threat
6 to national security or border security;

7 ''(2) provide capabilities, including training and
8 equipment, to partner countries to voluntarily collect
9 biometric and biographic identification data from in-
10 dividuals to identify, prevent, detect, and interdict
11 high risk individuals identified as national security,
12 border security, or terrorist threats who may at-
13 tempt to enter the United States utilizing illicit
14 pathways;

15 ''(3) provide capabilities, including training and
16 equipment, to partner countries to compare foreign
17 data against appropriate United States national se-
18 curity, border security, terrorist, immigration, and
19 counter-terrorism data, including—

20 ''(A) the Federal Bureau of Investigation's
21 Terrorist Screening Database, or successor
22 database;

23 ''(B) the Federal Bureau of Investigation's
24 Next Generation Identification database, or suc-
25 cessor database;

"(C) the Department of Defense Automated Biometric Identification System (commonly known as 'ABIS'), or successor database;

"(D) the Department's Automated Biometric Identification System (commonly known as 'IDENT'), or successor database; and

"(E) any other database, notice, or means that the Secretary, in consultation with the heads of other Federal departments and agencies responsible for such databases, notices, or means, designates;

"(4) provide partner countries with training, guidance, and best practices recommendations regarding the enrollment of individuals in BITMAP; and

"(5) ensure biometric and biographic identification data collected pursuant to BITMAP are incorporated into appropriate United States Government databases, in compliance with the policies and procedures established by the Privacy Officer appointed under section 222.

"(c) COLLABORATION.—The Secretary shall ensure that BITMAP operations include participation from relevant components of the Department, and request participation from other Federal agencies, as appropriate. Not-

1 withstanding any other provision of law, the Secretary
2 may enter into agreements related to such participation
3 on a reimbursable or non-reimbursable basis, as appro-
4 priate.

5 ''(d) AGREEMENTS.—Before carrying out BITMAP
6 operations in a foreign country that, as of the date of the
7 enactment of this section, was not a partner country de-
8 scribed in this section, the Secretary, in consultation with
9 the Secretary of State, shall enter into agreement or ar-
10 rangement with the government of such country that sets
11 forth program goals for such country, includes training,
12 guidance, and best practices recommendations regarding
13 the enrollment of individuals in BITMAP, and outlines
14 such operations in such country, including related depart-
15 mental operations. Such country shall be a partner coun-
16 try described in this section pursuant to and for purposes
17 of such agreement or arrangement.

18 ''(e) NOTIFICATION TO CONGRESS.—Not later than
19 60 days before an agreement or arrangement with the gov-
20 ernment of a foreign country to carry out BITMAP oper-
21 ations in such foreign country enters into force, the Sec-
22 retary shall provide the Committee on Homeland Security
23 of the House of Representatives and the Committee on
24 Homeland Security and Governmental Affairs of the Sen-

ate with a copy of such agreement or arrangement to establish such operations, including the following:

"(1) The identification of the foreign country with which the Secretary intends to enter into such an agreement or arrangement.

"(2) The location at which such operations will be conducted.

"(3) Goals for BITMAP operations in the foreign country.

"(4) The terms and conditions for Department personnel operating at such location.

"(f) CAPTURED INFORMATION OF UNITED STATES CITIZENS.—The Secretary shall ensure that any biometric and biographic identification data of United States citizens that is captured by BITMAP operations is expunged from all databases to which such data was uploaded, unless such data is retained for specific law enforcement or intelligence purposes.".

(b) REPORT.—Not later than 180 days after the date on which the Biometric Identification Transnational Migration Alert Program (BITMAP) is established under section 447 of the Homeland Security Act of 2002 (as added by subsection (a) of this section) and annually thereafter for the following five years, the Secretary of Homeland Security shall submit to the Committee on

1 Homeland Security of the House of Representatives and
2 the Committee on Homeland Security and Governmental
3 Affairs of the Senate a report that—
4 (1) outlines the strategic goals and operational
5 plans for BITMAP;
6 (2) outlines key efforts and the progress made
7 with each partner country;
8 (3) provides a description of the agreement or
9 arrangement with the government of each partner
10 country, if practicable;
11 (4) provides budget information related to ex-
12 penditures in support of BITMAP, including the
13 source of funding and anticipated expenditures;
14 (5) sets forth Department of Homeland Secu-
15 rity personnel, equipment, and infrastructure sup-
16 port to be used by BITMAP, broken down by coun-
17 try and number;
18 (6) includes the number of individuals each
19 partner country enrolled into BITMAP during the
20 reporting period, broken down by key categories, as
21 determined by U.S. Immigration and Customs En-
22 forcement;
23 (7) includes the training, guidance, and best
24 practices recommendations provided pursuant to
25 subsection (b)(4) of such section 447;

(8) includes a review of the redress process for BITMAP; and

(9) details the effectiveness of BITMAP operations in enhancing national security, border security, and counterterrorism operations.

(c) BRIEFINGS.—Not later than 30 days after each report is submitted pursuant to subsection (b), the Secretary of Homeland Security shall brief the Committee on Homeland Security and Governmental Affairs of the Senate and the Committee on Homeland Security of the House of Representatives regarding—

(1) individuals enrolled in BITMAP who have been apprehended at the United States border or in the interior of the United States; and

(2) asylum claims that were submitted by individuals who are enrolled in BITMAP.

(d) 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 444 the following new item:

"Sec. 445. Biometric Identification Transnational Migration Alert Program.".

SEC. 420. REPORTING OF VISA OVERSTAYS.

Section 2 of Public Law 105–173 (8 U.S.C. 1376) is amended—

(1) in subsection (a)—

(A) by striking ''Attorney General'' and inserting ''Secretary of Homeland Security''; and

(B) by inserting before the period at the end the following: '', and any additional information that the Secretary determines necessary for purposes of the report under subsection (b)'';

(2) by amending subsection (b) to read as follows:

''(b) ANNUAL REPORT.—Not later than September 30, 2021, and not later than September 30 of each year thereafter, the Secretary of Homeland Security shall submit to the Committee on Homeland Security and the Committee on the Judiciary of the House of Representatives and to the Committee on Homeland Security and Governmental Affairs and the Committee on the Judiciary of the Senate a report providing, for the preceding fiscal year, numerical estimates (including information on the methodology utilized to develop such numerical estimates) of the following:

''(1) For each country, the number of aliens from the country who are described in subsection (a), including the following:

''(A) The total number of such aliens within all classes of nonimmigrant aliens described

in section 101(a)(15) of the Immigration and Nationality Act (8 U.S.C. 1101(a)(15)).

''(B) The number of such aliens within each of the classes of nonimmigrant aliens, as well as the number of such aliens within each of the subclasses of such classes of nonimmigrant aliens, as applicable.

''(2) For each country, the percentage of the total number of aliens from the country who were present in the United States and were admitted to the United States as nonimmigrants who are described in subsection (a).

''(3) The number of aliens described in subsection (a) who arrived by land at a port of entry into the United States.

''(4) The number of aliens described in subsection (a) who entered the United States using a border crossing identification card (as such term is defined in section 101(a)(6) of the Immigration and Nationality Act (8 U.S.C. 1101(a)(6))).

''(5) The number of Canadian nationals who entered the United States without a visa whose authorized period of stay in the United States terminated during the previous fiscal year, but who remained in the United States.''.

SEC. 421. STUDENT AND EXCHANGE VISITOR INFORMATION SYSTEM VERIFICATION.

Not later than 90 days after the date of the enactment of this Act, the Secretary of Homeland Security shall ensure that the information collected under the program established under section 641 of the Illegal Immigration Reform and Immigrant Responsibility Act of 1996 (8 U.S.C. 1372) is available to officers of U.S. Customs and Border Protection for the purpose of conducting primary inspections of aliens seeking admission to the United States at each port of entry of the United States.

SEC. 422. SOCIAL MEDIA REVIEW OF VISA APPLICANTS.

(a) IN GENERAL.—Subtitle D of title IV of the Homeland Security Act of 2002 (6 U.S.C. 231 et seq.), as amended by this title, is further amended by adding at the end the following new sections:

"SEC. 446. SOCIAL MEDIA SCREENING.

''(a) IN GENERAL.—Not later than 180 days after the date of the enactment of this section, the Secretary shall, to the greatest extent practicable, and in a risk based manner and on an individualized basis, begin reviewing the social media accounts of certain visa applicants who are citizens of, or who reside in, high-risk countries, as determined by the Secretary based on the criteria described in subsection (b).

1 "(b) HIGH-RISK CRITERIA DESCRIBED.—In deter-
2 mining whether a country is high-risk pursuant to sub-
3 section (a), the Secretary, in consultation with the Sec-
4 retary of State, shall consider the following criteria:
5 "(1) The number of nationals of the country
6 who were identified in United States Government
7 databases related to the identities of known or sus-
8 pected terrorists during the previous year.
9 "(2) The level of cooperation of the country
10 with the counter-terrorism efforts of the United
11 States.
12 "(3) The number of counterintelligence, intel-
13 lectual property theft, and counterproliferation cases
14 involving nationals of the country.
15 "(4) Any other criteria the Secretary deter-
16 mines appropriate.
17 "(c) COLLABORATION.—To carry out the require-
18 ments of subsection (a), the Secretary may collaborate
19 with the following:
20 "(1) The head of a national laboratory within
21 the Department's laboratory network with relevant
22 expertise.
23 "(2) The head of a relevant university-based
24 center within the Department's centers of excellence
25 network.

1 ''(3) The heads of other appropriate Federal
2 agencies.
3 ''(d) WAIVER.—The Secretary, in collaboration with
4 the Secretary of State, is authorized to waive the require-
5 ments of subsection (a) as necessary to comply with inter-
6 national obligations of the United States.

7 **''SEC. 447. OPEN SOURCE SCREENING.**

8 ''The Secretary shall, to the greatest extent prac-
9 ticable, and in a risk based manner, review open source
10 information of visa applicants.''.
11 (b) CLERICAL AMENDMENT.—The table of contents
12 in section 1(b) of the Homeland Security Act of 2002, is
13 amended by inserting after the item relating to section
14 445, as added by this title, the following new items:

''Sec. 446. Social media screening.
''Sec. 447. Open source screening.''.

15 **SEC. 423. HOMELAND SECURITY INVESTIGATIONS NA-**
16 **TIONAL GANG UNIT.**

17 (a) IN GENERAL.—Subtitle D of title IV of the
18 Homeland Security Act of 2002 (6 U.S.C. 231 et seq.),
19 as amended by this title, is further amended by adding
20 at the end the following new section:

21 **''SEC. 448. NATIONAL GANG UNIT.**

22 ''(a) ESTABLISHMENT.—There is established within
23 the Department a program, which shall be known as the
24 'Homeland Security Investigations National Gang Unit'

1 (referred to in this section as 'National Gang Unit'. The
2 National Gang Unit shall be headed by an Assistant Di-
3 rector, who shall be appointed by the Executive Associate
4 Director of United States Immigration and Customs En-
5 forcement, Homeland Security Investigations.

6 ''(b) PURPOSE.—The purpose of the National Gang
7 Unit shall be to—

8 ''(1) lead homeland security investigations into
9 transnational criminal gang activity; and

10 ''(2) form partnerships with regional stake-
11 holders to target gangs, suppress violence and pros-
12 ecute criminal enterprises.

13 ''(c) TASK FORCES.—The National Gang Unit shall
14 establish and lead regionally based task force units fo-
15 cused on combating transnational gang activity. Such task
16 force units shall incorporate the following:

17 ''(1) Homeland Security Investigations per-
18 sonnel.

19 ''(2) School Resource Officers.

20 ''(3) State and local law enforcement.

21 ''(4) Personnel from other relevant agencies or
22 organizations.

23 ''(d) INFORMATION SHARING.—

24 ''(1) PROVIDED TO HOMELAND SECURITY.—Be-
25 fore placing an unaccompanied alien child with an

individual, the Secretary of Health and Human Services shall provide to the Secretary of Homeland Security any disclosed gang affiliation information the unaccompanied alien child provided to the Department of Health and Human Services, including factual information provided by employees and contractors of the Department related to patterns of violent behavior or suspected gang affiliation while under their supervision.

"(2) PROVIDED TO THE NATIONAL GANG UNIT.—The Secretary of Homeland Security shall share the information provided pursuant to paragraph (1) with relevant National Gang Unit task force units.

"(e) EFFECTIVE DATE.—This section shall apply to any unaccompanied alien child apprehended on or after the date of the enactment of this section.

"(f) AUTHORIZATION OF APPROPRIATIONS.—There is authorized to be appropriated $5,000,000 for each of fiscal years 2021 and 2022 to carry out 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 447, as added by this title, the following new item:

"Sec. 448. National Gang Unit.".

SEC. 424. HOMELAND SECURITY INVESTIGATIONS TRANSNATIONAL CRIMINAL INVESTIGATIVE UNITS.

(a) IN GENERAL.—Subtitle D of title IV of the Homeland Security Act of 2002 (6 U.S.C. 231 et seq.), as amended by this title, is further amended by adding at the end the following new section:

"SEC. 449. TRANSNATIONAL CRIMINAL INVESTIGATIVE UNITS.

"(a) ESTABLISHMENT.—There is established within the Department a program, which shall be known as the 'Homeland Security Investigations Transnational Criminal Investigative Unit Program' (referred to in this section as 'TCIU Program'). The TCIU Program shall be headed by an Assistant Director, who shall be appointed by the Executive Associate Director of U.S. Immigration and Customs Enforcement, Homeland Security Investigations.

"(b) PURPOSE.—The purpose of the TCIU Program shall be to—

"(1) lead homeland security investigations into transnational criminal organizations; and

"(2) enhance cooperation between Homeland Security Investigations and trusted and vetted foreign law enforcement partners in order to identify targets, collect evidence, share information, and facilitate the prosecution of transnational criminal or-

ganizations both in-country and through the United States judicial system.

''(c) AUTHORIZATION OF APPROPRIATIONS.—There is authorized to be appropriated, $5,000,000 for each of fiscal years 2021 and 2022 to carry out 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 448, as added by this title, the following new item:

''Sec. 449. Transnational criminal investigative unit program.''.

SEC. 425. HOMELAND SECURITY INVESTIGATIONS INNOVATION LAB.

(a) IN GENERAL.—Subtitle D of title IV of the Homeland Security Act of 2002 (6 U.S.C. 231 et seq.), as amended by this title, is further amended by adding at the end the following new section:

''SEC. 450. INNOVATION LAB.

''(a) ESTABLISHMENT.—There is established within the Department a program, which shall be known as the 'Homeland Security Investigations Innovation Lab' (referred to in this section as 'Innovation Lab'. The Innovation Lab shall be headed by an Assistant Director, who shall be appointed by the Executive Associate Director of United States Immigration and Customs Enforcement, Homeland Security Investigations.

1 ''(b) PURPOSE.—The purpose of the Innovation Lab
2 shall be to improve investigative efficiency and mission-
3 critical outcomes by enhancing and streamlining data
4 processing, agility, assessment, visualization, and analysis
5 of homeland security data, using innovative and emerging
6 technologies and best practices for design principles. Inno-
7 vation Lab efforts shall be informed by designated field
8 agents and analysts with relevant experience.
9 ''(c) CO-LOCATION.—The Secretary of Homeland Se-
10 curity shall, if practicable, co-locate Innovation Lab per-
11 sonnel and office space with other existing assets of—
12 ''(1) the Department of Homeland Security,
13 where possible; or
14 ''(2) Federal facilities, where appropriate.
15 ''(d) COMPOSITION.—The Innovation Lab shall be
16 comprised of personnel from the following:
17 ''(1) Homeland Security Investigations of U.S.
18 Immigration and Customs Enforcement.
19 ''(2) Other appropriate agencies as determined
20 by the Secretary.
21 ''(3) The private sector, including developers
22 with specializations in innovative and emerging tech-
23 nology, back end architecture, or user interface de-
24 sign.

"(4) Academic institutions, including members of the Department of Homeland Security Centers of Excellence.

"(e) PRIORITIZATION.—The Innovation Lab shall prioritize new projects based on communicated investigative challenges experienced by each Homeland Security Investigations field office. Such communication may be incorporated in existing annual threat analyses conducted by Homeland Security Investigations.

"(f) AUTHORIZATION OF APPROPRIATIONS.—There is authorized to be appropriated $24,700,000 for fiscal year 2021 and $27,700,000 for fiscal year 2022 to carry out 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 449, as added by this title, the following new item:

"Sec. 450. Homeland security investigations innovation lab.".

SEC. 426. ESTABLISHMENT OF UNITED STATES CITIZENSHIP AND IMMIGRATION SERVICES.

(a) IN GENERAL.—Section 451 of the Homeland Security Act of 2002 (6 U.S.C. 271) is amended to read as follows:

"SEC. 451. UNITED STATES CITIZENSHIP AND IMMIGRATION SERVICES.

"(a) ESTABLISHMENT.—There is established within the Department an agency to be known as United States Citizenship and Immigration Services.

"(b) DIRECTOR OF UNITED STATES CITIZENSHIP AND IMMIGRATION SERVICES.—There shall be at the head of United States Citizenship and Immigration Services a Director of United States Citizenship and Immigration Services (in this section referred to as the 'Director').

"(c) DUTIES AND QUALIFICATIONS.—The Director shall—

"(1) have a minimum of five years of management experience;

"(2) establish national immigration services policies and priorities;

"(3) meet regularly with the Citizenship and Immigration Services Ombudsman (established in section 452) to correct serious problems identified by such Ombudsman;

"(4) advise the Secretary with respect to any policy or operation of United States Citizenship and Immigration Services that may significantly affect another component or office of the Department;

"(5) carry out—

1 "(A) the adjudication of nonimmigrant and
2 immigrant visa petitions;
3 "(B) the adjudication of naturalization ap-
4 plications;
5 "(C) the adjudication of asylum and ref-
6 ugee applications;
7 "(D) adjudications performed at United
8 States Citizenship and Immigration Services
9 service centers; and
10 "(E) all other adjudications formerly per-
11 formed pursuant to this section by the Immi-
12 gration and Naturalization Service, the Bureau
13 of Citizenship and Immigration Services, or
14 United States Citizenship and Immigration
15 Services, as the case may be, on the day before
16 the date of the enactment of this section; and
17 "(6) carry out other duties and powers pre-
18 scribed by law or delegated by the Secretary.
19 "(d) DEPUTY DIRECTOR.—There shall be in United
20 States Citizenship and Immigration Services a Deputy Di-
21 rector, who shall assist the Director in the management
22 of United States Citizenship and Immigration Services.
23 "(e) CHIEF COUNSEL.—There shall be in United
24 States Citizenship and Immigration Services a Chief
25 Counsel, who shall—

1 ''(1) provide specialized legal advice, opinions,
2 determinations, and any other assistance to the Di-
3 rector with respect to legal matters affecting United
4 States Citizenship and Immigration Services;
5 ''(2) represent United States Citizenship and
6 Immigration Services in visa petition appeal pro-
7 ceedings before the Executive Office for Immigration
8 Review; and
9 ''(3) carry out other duties and powers pre-
10 scribed by the Secretary.
11 ''(f) CHIEF OF POLICY AND STRATEGY.—There shall
12 be in United States Citizenship and Immigration Services
13 a Chief of Policy and Strategy, who shall—
14 ''(1) make policy recommendations and perform
15 policy research and analysis on immigration services
16 issues;
17 ''(2) coordinate immigration policy issues with
18 other appropriate components and offices of the De-
19 partment; and
20 ''(3) carry out other duties and powers pre-
21 scribed by the Secretary.
22 ''(g) OFFICE OF CITIZENSHIP.—
23 ''(1) IN GENERAL.—There is established in
24 United States Citizenship and Immigration Services
25 the Office of Citizenship.

1 "(2) CHIEF.—There shall be at the head of the
2 Office of Citizenship a Chief, who shall report to the
3 Director.
4 "(3) DUTIES.—The Chief of the Office of Citi-
5 zenship shall—
6 "(A) promote instruction and training on
7 citizenship responsibilities, including the devel-
8 opment of education materials and develop ini-
9 tiatives to foster the civic integration of immi-
10 grants, for aliens interested in becoming natu-
11 ralized citizens of the United States; and
12 "(B) carry out other duties and powers
13 prescribed by the Director.
14 "(h) FRAUD DETECTION AND NATIONAL SECURITY
15 DIRECTORATE.—
16 "(1) IN GENERAL.—There is established in
17 United States Citizenship and Immigration Services
18 a Fraud Detection and National Security Direc-
19 torate.
20 "(2) ASSOCIATE DIRECTOR.—There shall be at
21 the head of the Fraud Detection and National Secu-
22 rity Directorate an Associate Director, who shall re-
23 port to the Director.

1 "(3) DUTIES.—The Associate Director of the
2 Fraud Detection and National Security Directorate
3 shall—
4 "(A) ensure immigration benefits are not
5 granted to individuals who—
6 "(i) pose a threat to national security
7 or public safety;
8 "(ii) are known or suspected terror-
9 ists; or
10 "(iii) seek to defraud or have pre-
11 viously sought to or have defrauded the
12 immigration system of the United States;
13 "(B) conduct security and background in-
14 vestigations of applicants for immigration bene-
15 fits and develop systems and techniques for
16 identifying immigration benefit fraud;
17 "(C) conduct targeted site visits in cases in
18 which fraud is suspected;
19 "(D) investigate and refer to U.S. Immi-
20 gration and Customs Enforcement, where ap-
21 propriate, incidents of suspected fraud, national
22 security concerns, or other civil and criminal
23 violations of immigration laws; and
24 "(E) carry out other duties and powers
25 prescribed by the Director.

1 "(i) FIELD OPERATIONS DIRECTORATE.—
2 "(1) IN GENERAL.—There is established in
3 United States Citizenship and Immigration Services
4 a Field Operations Directorate.
5 "(2) ASSOCIATE DIRECTOR.—There shall be at
6 the head of the Field Operations Directorate an As-
7 sociate Director, who shall report to the Director.
8 "(3) DUTIES.—The Associate Director of the
9 Field Operations Directorate shall—
10 "(A) oversee the domestic regional offices,
11 district offices, field offices, and field support
12 offices of United States Citizenship and Immi-
13 gration Services;
14 "(B) adjudicate applications and petitions
15 for immigration benefits;
16 "(C) interview applicants for immigration
17 benefits;
18 "(D) conduct security and background in-
19 vestigations of applicants for immigration bene-
20 fits and develop systems and techniques for
21 identifying immigration benefit fraud; and
22 "(E) carry out other duties and powers
23 prescribed by the Director.
24 "(j) REFUGEE, ASYLUM, AND INTERNATIONAL OP-
25 ERATIONS DIRECTORATE.—

1 "(1) IN GENERAL.—There is established in
2 United States Citizenship and Immigration Services
3 a Refugee, Asylum, and International Operations
4 Directorate.
5 "(2) ASSOCIATE DIRECTOR.—There shall be at
6 the head of the Refugee, Asylum, and International
7 Operations Directorate an Associate Director, who
8 shall report to the Director.
9 "(3) DUTIES.—The Associate Director of the
10 Refugee, Asylum, and International Operations Di-
11 rectorate shall—
12 "(A) adjudicate asylum and refugee appli-
13 cations;
14 "(B) conduct screenings on individuals
15 seeking to enter the United States and mi-
16 grants interdicted at sea;
17 "(C) adjudicate parole requests from indi-
18 viduals residing outside the United States for
19 humanitarian or public benefit reasons;
20 "(D) perform other authorized functions of
21 United States Citizenship and Immigration
22 Services outside the United States;
23 "(E) conduct security and background in-
24 vestigations of applicants for immigration bene-

fits and develop systems and techniques for identifying immigration benefit fraud; and

"(F) carry out other duties and powers prescribed by the Director.

"(k) IMMIGRATION RECORD AND IDENTITY SERVICES DIRECTORATE.—

"(1) IN GENERAL.—There is established in United States Citizenship and Immigration Services an Immigration Records and Identity Services Directorate.

"(2) ASSOCIATE DIRECTOR.—There shall be at the head of the Immigration Records and Identity Services Directorate an Associate Director, who shall report to the Director.

"(3) DUTIES.—The Associate Director of the Immigration Records and Identity Services Directorate shall—

"(A) collect and disseminate biometric information to support the integrity of the immigration system;

"(B) manage the employment verification system pursuant to 404(a) of the Illegal Immigration Reform and Immigrant Responsibility Act of 1996 (8 U.S.C. 1324a note), or successor provision;

1 "(C) manage the automated system known
2 as the Systematic Alien Verification for Entitle-
3 ments, or successor system, to assist Federal,
4 State, and local benefit issuing agencies to de-
5 termine the immigration status of benefit appli-
6 cants;
7 "(D) provide appropriate information, in-
8 cluding immigration status and employment au-
9 thorization information, to relevant customers
10 and stakeholders; and
11 "(E) carry out other duties and powers
12 prescribed by the Director.
13 "(l) SERVICE CENTER OPERATIONS DIREC-
14 TORATE.—
15 "(1) IN GENERAL.—There is established in
16 United States Citizenship and Immigration Services
17 a Service Center Operations Directorate.
18 "(2) ASSOCIATE DIRECTOR.—There shall be at
19 the head of the Service Center Operations Direc-
20 torate an Associate Director, who shall report to the
21 Director.
22 "(3) DUTIES.—The Associate Director of the
23 Service Center Operations Directorate shall—
24 "(A) oversee the adjudication of employ-
25 ment-based applications and petitions at United

States Citizenship and Immigration Services service centers;

"(B) conduct security and background investigations of applicants for immigration benefits and develop systems and techniques for identifying immigration benefit fraud;

"(C) manage the employment creation visa program under section 203(b)(5) of the Immigration and Nationality Act (8 U.S.C. 1153(b)(5)); and

"(D) carry out other duties and powers prescribed by the Director.

"(m) OTHER AUTHORITIES.—

"(1) IN GENERAL.—The Secretary may establish such other Associate Directors, or other similar positions or officials, as the Secretary determines necessary to carry out the missions, duties, functions, and authorities of United States Citizenship and Immigration Services.

"(2) NOTIFICATION.—If the Secretary exercises the authority provided pursuant to paragraph (1), the Secretary shall notify the Committee on Homeland Security and the Committee on the Judiciary of the House of Representatives and the Committee on Homeland Security and Governmental Affairs and

the Committee on the Judiciary of the Senate not later than 30 days before exercising such authority.''.

(b) SPECIAL RULES.—

(1) TREATMENT.—Section 451 of the Homeland Security Act of 2002 (6 U.S.C. 271), as amended by subsection (a) of this section, shall be treated as if included in such Act as of the date of the enactment of such Act. In addition to the functions, missions, duties, and authorities specified in such amended section 451, United States Citizenship and Immigration Services shall continue to perform and carry out the functions, missions, duties, and authorities under section 451 of such Act as in existence on the day before such date of enactment (notwithstanding the treatment described in this paragraph).

(2) RULES OF CONSTRUCTION.—

(A) RULES AND REGULATIONS.—Notwithstanding the treatment described in paragraph (1), nothing in this Act may be construed as affecting in any manner any rule or regulation issued or promulgated pursuant to any provision of law, including section 451 of the Homeland Security Act of 2002 (6 U.S.C. 271), as

in existence on the day before the date of the enactment of this Act, and any such rule or regulation shall continue to have full force and effect on and after such date.

(B) OTHER ACTIONS.—Notwithstanding the treatment described in paragraph (1), nothing in this Act may be construed as affecting in any manner any action, determination, policy, or decision pursuant to section 451 of the Homeland Security Act of 2002 (6 U.S.C. 271) as in existence on the day before the date of the enactment of this Act, and any such action, determination, policy, or decision shall continue to have full force and effect on and after such date.

(c) CONTINUATION IN OFFICE.—

(1) DIRECTOR.—The individual serving as Director of United States Citizenship and Immigration Services on the day before the date of the enactment of this Act may, notwithstanding the treatment provision under paragraph (1) of subsection (b), continue to serve as the Director of United States Citizenship and Immigration Services on and after such date of enactment in accordance with section 451 of the Homeland Security Act of 2002 (6 U.S.C. 271),

as amended by subsection (a) of this section, until the earlier of—

(A) the date on which such individual is no longer eligible to serve as Director; or

(B) the date on which a person nominated by the President to be the Director is confirmed by the Senate in accordance with such amended section 451.

(2) OTHER POSITIONS.—The individuals serving as Chiefs, Associate Directors and other officers and officials under section 451 of the Homeland Security Act of 2002 (6 U.S.C. 271) on the day before the date of the enactment of this Act may, notwithstanding the treatment provision under paragraph (1) of subsection (b), serve as the appropriate Chiefs, Assistant Directors and other officers and officials under such section 451 as amended by subsection (a) of this section unless the Director of United States Citizenship and Immigration Services determines that another individual should hold such position.

(d) REFERENCES.—

(1) TITLE 5.—Section 5314 of title 5, United States Code, is amended by striking ''Director of the Bureau of Citizenship and Immigration Services''

and inserting ''Director of United States Citizenship and Immigration Services, Department of Homeland Security''.

(2) OTHER REFERENCES.—On and after the date of the enactment of this Act, any reference in any other Federal law, Executive order, rule, regulation, or delegation of authority to the ''Director of the Bureau of Citizenship and Immigration Services'' or the ''Bureau of Citizenship and Immigration Services'' shall be deemed to be a reference to the Director of United States Citizenship and Immigration Services or United States Citizenship and Immigration Services, respectively.

(e) CLERICAL AMENDMENT.—The table of contents in section 1(b) of such Act is amended by amending the item relating to section 451 to read as follows:

''Sec. 451. United States Citizenship and Immigration Services.''.

(f) CONFORMING AMENDMENTS.—The Homeland Security Act of 2002 is amended—

(1) in subparagraph (E) of section 103(a) (6 U.S.C. 113(a)), by striking ''A Director of the Bureau of Citizenship and Immigration Services'' and inserting ''A Director of United States Citizenship and Immigration Services'';

(2) in section 452 (6 U.S.C. 272)—

(A) in paragraphs (1), (2), and (3) of subsection (b), by striking ''the Bureau of Citizenship and Immigration Services'' each place it appears and inserting ''United States Citizenship and Immigration Services'';

(B) in subsection (c)—

(i) in subparagraphs (A) and (E) of paragraph (1), by striking ''the Bureau of Citizenship and Immigration Services'' each place it appears and inserting ''United States Citizenship and Immigration Services''; and

(ii) in paragraph (2), by striking ''Director of the Bureau of Citizenship and Immigration Services'' and inserting ''Director of United States Citizenship and Immigration Services'';

(C) in subsection (d)—

(i) in paragraph (2), by striking ''the Bureau of Citizenship and Immigration Services'' and inserting ''United States Citizenship and Immigration Services''; and

(ii) paragraph (4), by striking ''Director of the Bureau of Citizenship and Immi-

gration Services'' and inserting ''Director of United States Citizenship and Immigration Services'';

(D) in paragraph (2) of subsection (e), by striking ''the Bureau of Citizenship and Immigration Services'' and inserting ''United States Citizenship and Immigration Services'';

(E) in subsection (f)—

(i) in the heading, by striking ''BUREAU OF CITIZENSHIP AND IMMIGRATION SERVICES'' and inserting ''UNITED STATES CITIZENSHIP AND IMMIGRATION SERVICES''; and

(ii) by striking ''Director of the Bureau of Citizenship and Immigration Services'' and inserting ''Director of United States Citizenship and Immigration Services''; and

(F) in subsection (g)—

(i) in subparagraphs (B) and (D) of paragraph (1), by striking ''the Bureau of Citizenship and Immigration Services'' each place it appears and inserting ''United States Citizenship and Immigration Services''; and

(ii) in paragraph (2), by striking ''the Bureau of Citizenship and Immigration Services'' each place it appears and inserting ''United States Citizenship and Immigration Services'';

(3) in section 453 (6 U.S.C. 273)—

(A) in subsection (a)—

(i) in the matter preceding paragraph (1), by striking ''Director of the Bureau of Citizenship and Immigration Services'' and inserting ''Director of United States Citizenship and Immigration Services'';

(ii) in paragraphs (1) and (3), by striking ''the Bureau of Citizenship and Immigration Services'' each place it appears and inserting ''United States Citizenship and Immigration Services''; and

(iii) in paragraph (2)—

(I) by striking ''the Bureau of Citizenship and Immigration Services'' and inserting ''United States Citizenship and Immigration Services''; and

(II) by striking ''such bureau'' and inserting ''United States Citizenship and Immigration Services''; and

(B) in subsection (b), in the matter preceding paragraph (1), by striking ''Bureau of Citizenship and Immigration Services'' and inserting ''United States Citizenship and Immigration Services'';

(4) in section 456 (6 U.S.C. 275) by striking ''Director of the Bureau of Citizenship and Immigration Services'' each place it appears and inserting ''Director of United States Citizenship and Immigration Services'';

(5) in subparagraph (A) of section 462(b)(2) (6 U.S.C. 279(b)(2)), by striking ''Director of the Bureau of Citizenship and Immigration Services'' and inserting ''Director of United States Citizenship and Immigration Services'';

(6) in subsections (a), (b), and (d) of section 476 (6 U.S.C. 296), by striking ''the Bureau of Citizenship and Immigration Services'' each place it appears and inserting ''United States Citizenship and Immigration Services''; and

(7) in section 478 (6 U.S.C. 298)—

(A) by striking subsection (b);

(B) by striking the following:

''(a) ANNUAL REPORT.—

''(1) IN GENERAL.—One year after'';

(C) by inserting the following:

''(a) IN GENERAL.—One year after'';

(D) by striking the following:

''(2) MATTER INCLUDED.—The report shall'';

(E) by inserting the following:

''(b) MATTER INCLUDED.—The report shall'';

(F) by redesignating subparagraphs (A) through (H) as paragraphs (1) through (8), respectively; and

(G) by striking ''The Department of Justice'' in new paragraph (5) and replacing it with ''The Department of Homeland Security''.

(g) REPEALS.—

(1) IN GENERAL.—The following provisions of the Homeland Security Act of 2002 are repealed:

(A) Section 459 (6 U.S.C. 276).

(B) Section 460 (6 U.S.C. 277).

(C) Section 461 (6 U.S.C. 278).

(D) Section 472 (6 U.S.C. 292).

(E) Section 473 (6 U.S.C. 293).

(F) Section 474 (6 U.S.C. 294).

(G) Section 475 (6 U.S.C. 295).

(H) Section 477 (6 U.S.C. 297).

(2) CLERICAL AMENDMENTS.—The table of contents in section 1(b) of the Homeland Security Act of 2002 is amended by striking the items relating to the following sections:

(A) Section 459.

(B) Section 460.

(C) Section 461.

(D) Section 472.

(E) Section 473.

(F) Section 474.

(G) Section 475.

(H) Section 477.

(h) EMPLOYEE DISCIPLINE.—Section 454 of the Homeland Security Act of 2002 (6 U.S.C. 274) is amended to read as follows:

"SEC. 454. EMPLOYEE DISCIPLINE.

''Notwithstanding any other provision of law, the Secretary may impose disciplinary action on any employee of United States Citizenship and Immigration Services who knowingly deceives Congress or agency leadership on any matter.''.

(i) COMBINATION PROHIBITION.—

(1) IN GENERAL.—Section 471 of the Homeland Security Act of 2002 (6 U.S.C. 291) is amended to read as follows:

"SEC. 471. COMBINATION PROHIBITION.

''The authority provided by section 1502 may be used to reorganize functions or organizational units within U.S. Immigration and Customs Enforcement or United States Citizenship and Immigration Services, but may not be used to combine the two components into a single agency or otherwise to combine, join, or consolidate functions or organizational units of the two components with each other.''.

(2) CLERICAL AMENDMENT.—The table of contents in section 1(b) of the Homeland Security Act of 2002 is amended by amending the item relating to section 471 to read as follows:

''Sec. 471. Combination prohibition.''.

SEC. 427. FRAUD PREVENTION.

(a) PROSPECTIVE ANALYTICS TECHNOLOGY.—

(1) PLAN FOR IMPLEMENTATION.—Not later than 180 days after the date of the enactment of this Act, the Secretary of Homeland Security shall develop a plan to digitize the remaining paper biometrics files of past immigration benefits applications and use advanced analytics software to ensure the proactive detection of fraud in immigration bene-

fits applications and petitions and to ensure that any such applicant or petitioner does not pose a threat to national security.

(2) IMPLEMENTATION OF PLAN.—Not later than one year after the date of the submission of the plan under subsection (1), the Secretary of Homeland Security shall begin implementation of the plan.

SEC. 428. BORDER SECURITY AND TRADE MODERNIZATION TRUST FUND.

(a) BORDER SECURITY TRUST FUND.—Subtitle C of title IV of the Homeland Security Act of 2002, as amended by this title, is further amended by adding at the end the following new section:

"SEC. 438. BORDER SECURITY AND TRADE MODERNIZATION TRUST FUND.

''(a) ESTABLISHMENT.—There is hereby established in the Treasury of the United States a trust fund to be known as the 'Border Security and Trade Modernization Trust Fund' (in this section referred to as the 'Fund').

''(b) DEPOSITS TO THE FUND.—There shall be deposited in the Fund the following:

''(1) Amounts authorized and appropriated to that Fund.

''(2) Surcharges established in subsection (f).

''(3) Gifts accepted pursuant to subsection (g).

1 ''(4) Penalties collected under subchapter II of
2 chapter 12 of title 8, United States Code.
3 ''(c) USE OF AMOUNTS IN FUND.—
4 ''(1) The Secretary may use amounts in the
5 fund without further appropriation to carry out the
6 following activities included in the Border Security
7 Improvement Plan submitted under section 439:
8 ''(A) acquisition, construction, and instal-
9 lation of physical barriers, tactical infrastruc-
10 ture, cameras, sensors and other technology.
11 ''(B) acquisition, construction, renovation,
12 and improvement of short-term detention facili-
13 ties used for processing of individuals detained
14 by U.S. Customs and Border Protection and
15 long-term detention facilities used for individ-
16 uals detained by U.S. Immigration and Cus-
17 toms Enforcement, including facilities to accom-
18 modate family units.
19 ''(C) acquisition, construction, renovation,
20 and improvement of port of entry facilities.
21 ''(2) Amounts in the fund shall remain available
22 until expended.
23 ''(d) LIMITATION ON EXPENDITURE.—

1 "(1) Amounts deposited in the Fund may not
2 be used for any activity except those provided for in
3 this section.
4 "(2) The Secretary may not expend amounts
5 from the Fund in any fiscal year in which the Bor-
6 der Security Improvement Plan has not been sub-
7 mitted pursuant to section 439.
8 "(e) LIMITATION ON OBLIGATION.—The Secretary
9 may not incur an obligation under a contract or other
10 agreement entered into to carry out an activity under this
11 section in excess of the unobligated balance, at the time
12 the contract or agreement is entered into, of the Fund
13 required to be used to satisfy the obligation.
14 "(f) BORDER SECURITY SURCHARGE.—
15 "(1) IN GENERAL.—Notwithstanding any other
16 provision of law,—
17 "(A) the Secretary shall charge a sur-
18 charge of
19 "(i) $40 on the immigrant user fee es-
20 tablished under section 286(m) of the Im-
21 migration and Nationality Act (8 U.S.C.
22 1356(m)); and
23 "(ii) $6 on the land border inspection
24 fee established under section 286(q) of
25 such Act (8 U.S.C. 1356(q)); and

"(B) the Secretary of State shall charge a surcharge of $20 on the machine-readable visa fee established under section 103 of the Enhanced Border Security and Visa Entry Reform Act of 2002 (8 U.S.C. 1713).

"(2) DEPOSIT OF SURCHARGES.—Surcharges collected under this subsection shall be deposited in the Fund established under this section.

"(g) ACCEPTANCE OF DONATIONS.—Notwithstanding section 3113 of title 31, the Secretary of the Treasury may accept for the Government a gift of money for deposit in the Fund.

"(h) SUNSET.—Amounts may not be deposited in the Fund and surcharges authorized under subsection (f) may not be collected on the date that is the sooner of—

"(1) the date on which the Secretary notifies the Committee on Homeland Security of the House of Representatives and the Committee on Homeland Security and Government Affairs of the Senate that amounts deposited in the Fund exceed $35,000,000,000; or

"(2) 15 years after the first date on which amounts are deposited in the Fund under subsection (b).".

(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 437, as added by this title, the following new item:

"Sec. 438. Border security and trade modernization trust fund.".

(c) CONFORMING AMENDMENT.—Notwithstanding any other provision of law, penalties collected under subchapter II of chapter 12 of title 8, United States Code, shall be deposited in the Border Security and Trade Modernization Trust Fund established under section 438 of the Homeland Security Act of 2002, as added by this section.

(d) AUTHORIZATION OF APPROPRIATIONS.—There are authorized to be appropriated to the Border Security and Trade Modernization Trust Fund established under section 438 of the Homeland Security Act of 2002, as added by this section, $4,500,000,000 for each of fiscal years 2021 and 2022.

SEC. 429. BORDER SECURITY IMPROVEMENT PLAN.

(a) IN GENERAL.—Subtitle C of title IV of the Homeland Security Act of 2002, as amended by this title, is further amended by adding at the end the following:

"SEC. 439. BORDER SECURITY IMPROVEMENT PLAN.

"(a) IN GENERAL.—On the date the President submits to Congress a budget pursuant to section 1105 of title 31, United States Code, the Secretary of Homeland

Security shall submit to the Committee on Homeland Security of the House of Representatives, the Committee on Homeland Security and Governmental Affairs of the Senate, and the Comptroller General of the United States a risk-based plan for improving security along the land borders of the United States.

''(b) TOPICS.—The plan required under subsection (a) shall include a needs assessment and prioritization of projects regarding the following:

''(1) Physical barriers, fencing, and tactical infrastructure.

''(2) Border Patrol mission-related technology including cameras, sensors, anti-tunnel detection, persistent surveillance and mobile and relocatable technologies.

''(3) Border Patrol access to the border including patrol roads and lighting.

''(4) Office of Field Operations mission-related port of entry technology including non-intrusive inspection systems.

''(5) Office of Field Operations port of entry and facility modernization.

''(6) Border Patrol interior checkpoint and facility modernization.

1 ''(7) Customs and Border Protection short-term
2 detention capacity.
3 ''(8) Immigration and Customs Enforcement
4 long-term detention facility capacity.
5 ''(c) ELEMENTS.—The plan required under sub-
6 section (a) shall include the following elements:
7 ''(1) A statement of goals, objectives, activities,
8 and milestones for the plan.
9 ''(2) A detailed implementation schedule for the
10 plan, including estimates for the planned obligation
11 of funds for the following five fiscal years that are
12 linked to the milestone-based delivery of specific—
13 ''(A) capabilities and services;
14 ''(B) mission benefits and outcomes;
15 ''(C) program management capabilities;
16 and
17 ''(D) lifecycle cost estimates.
18 ''(3) A description of the manner in which spe-
19 cific projects under the plan will enhance border se-
20 curity goals and objectives and address the highest
21 priority border security needs.
22 ''(4) An identification of the planned locations,
23 quantities, and types of projects considered under
24 the plan.

"(5) A description of the methodology and analyses used to inform the assessment conducted pursuant to subparagraph (b) for deployment to particular locations under the plan that includes the following:

"(A) Analyses of alternatives, where appropriate, including comparative costs and benefits.

"(B) An assessment of effects on relevant government and non-non-government stakeholders.

"(C) A description of other factors critical to the decision-making process.

"(6) An identification of staffing requirements under the plan, including full-time equivalents, contractors, and detailed personnel, disaggregated by activity.

"(7) A description of performance metrics for the plan for assessing and reporting on the contributions of border security capabilities realized from current and future investments.

"(8) A migrant surge response plan to improve the Department of Homeland Security response rate to future crises.

"(9) A description of the status of the actions of the Department of Homeland Security to address open recommendations by the Office of the Inspector

General of the Department and the Government Accountability Office relating to border security, including plans, schedules, and associated milestones for fully addressing such recommendations.

''(10) A plan to consult State and local elected officials on the eminent domain and construction process relating to physical barriers (except that such requirement may be satisfied through the submission of existing plans).

''(11) Certifications by the Under Secretary for Management of the Department of Homeland Security that—

''(A) the plan has been reviewed and approved in accordance with an acquisition review management process that complies with capital planning and investment control and review requirements established by the Office of Management and Budget, including as provided in Circular A–11, part 7; and

''(B) all activities under the plan comply with Federal acquisition rules, requirements, guidelines, and practices.

''(d) GAO EVALUATION.—Not later than 120 days after receipt of the plan required under subsection (a) by the Comptroller General of the United States, the Comp-

1 troller General shall evaluate the plan and report to the
2 Committee on Homeland Security of the House of Rep-
3 resentatives and the Committee on Homeland Security
4 and Governmental Affairs of the Senate on any concerns
5 or recommendations for improvement, as the Comptroller
6 General determines appropriate.''.

7 (b) CLERICAL AMENDMENT.—The table of contents
8 in section 1(b) of the Homeland Security Act of 2002 is
9 amended by inserting after the item relating to section
10 438, as added by this title, the following new item:

''Sec. 439. Border security improvement plan.''.

11 **SEC. 430. INTEGRATED BORDER ENFORCEMENT TEAMS.**

12 (a) IN GENERAL.—Subtitle C of title IV of the
13 Homeland Security Act of 2002 (6 U.S.C. 231 et seq.),
14 as amended by this title, is further amended by adding
15 at the end the following new section:

16 **''SEC. 440. INTEGRATED BORDER ENFORCEMENT TEAMS.**

17 ''(a) ESTABLISHMENT.—There is established within
18 the Department a program to be known as the Integrated
19 Border Enforcement Team program (referred to in this
20 section as 'IBET').

21 ''(b) PURPOSE.—The purpose of IBET is to enhance
22 border security in a manner that results in a cooperative
23 approach between the United States and Canada to—

24 ''(1) strengthen security between designated
25 ports of entry;

1 ''(2) detect, investigate, prevent, and respond to
2 terrorism, transnational criminal organizations, and
3 other violations of law related to border security;
4 ''(3) facilitate collaboration among components
5 and offices within the Department and international
6 partners;
7 ''(4) execute coordinated activities in further-
8 ance of border security and homeland security; and
9 ''(5) enhance information-sharing, including the
10 dissemination of homeland security information
11 among such components and offices.
12 ''(c) COMPOSITION AND ESTABLISHMENT OF
13 UNITS.—
14 ''(1) COMPOSITION.—IBET units may be com-
15 prised of personnel from the following:
16 ''(A) U.S. Customs and Border Protection.
17 ''(B) U.S. Immigration and Customs En-
18 forcement, led by Homeland Security Investiga-
19 tions.
20 ''(C) Other Department personnel, as ap-
21 propriate.
22 ''(D) Other Federal, State, local, Tribal,
23 and foreign law enforcement agencies, as appro-
24 priate.

1 "(E) Other appropriate personnel at the
2 discretion of the Secretary.
3 "(2) ESTABLISHMENT OF UNITS.—The Sec-
4 retary is authorized to establish IBET units in re-
5 gions in which such units can contribute to IBET
6 missions, as appropriate. When establishing an
7 IBET unit, the Secretary shall apply risk-based cri-
8 teria that takes into consideration the following:
9 "(A) Whether the region in which the
10 IBET unit would be established is significantly
11 impacted by cross-border threats, including
12 threats posed by transnational criminal organi-
13 zations and terrorist groups.
14 "(B) The availability of Federal, State,
15 local, Tribal, and foreign law enforcement re-
16 sources to participate in the IBET unit.
17 "(C) Whether, in accordance with para-
18 graph (3), other joint cross-border initiatives al-
19 ready take place within the region in which the
20 IBET unit would be established.
21 "(3) DUPLICATION OF EFFORTS.—In deter-
22 mining whether to establish a new IBET unit or to
23 expand an existing IBET unit in a given region, the
24 Secretary shall ensure that the IBET unit under
25 consideration does not duplicate the efforts of other

existing interagency task forces or centers within such region, including the Border Enforcement Security Task Force established under section 443.

"(d) OPERATION.—After determining the regions in which to establish IBET units under subsection (c)(2), the Secretary may—

"(1) direct the assignment of Federal personnel to such IBET units;

"(2) take other actions to assist Federal, State, local, and Tribal entities to participate in such IBET units, including providing financial assistance, as appropriate, for operational, administrative, and technological costs associated with such participation;

"(3) direct the development of policy and guidance necessary to identify, assess, and integrate the available partner resources in relevant border sector security assessments and resource planning documents;

"(4) establish targets and performance measures for such IBET units; and

"(5) direct leadership of such IBET units to monitor progress on such targets and performance measures.

1 "(e) COORDINATION.—The Secretary shall coordinate
2 IBET activities with other similar border security and
3 antiterrorism programs within the Department in accord-
4 ance with the strategic objectives of the Cross-Border Law
5 Enforcement Advisory Committee.

6 "(f) MEMORANDA OF UNDERSTANDING.—The Sec-
7 retary may enter into memoranda of understanding with
8 appropriate representatives of the entities specified in sub-
9 section (c)(1) as necessary to carry out this section. Such
10 memoranda with entities specified in subsection (c)(1)(G)
11 shall be entered into with the concurrence of the Secretary
12 of State.

13 "(g) REPORT.—Not later than 180 days after the
14 date on which IBET is established and biannually there-
15 after for the following six years, the Secretary shall submit
16 to the Committee on Homeland Security of the House of
17 Representatives and the Committee on Homeland Security
18 and Governmental Affairs of the Senate a report that—

19 "(1) describes the effectiveness of IBET units
20 in fulfilling the purposes specified in subsection (b);

21 "(2) identifies challenges on the sustainment of
22 cross-border IBET operations, including challenges
23 faced by international partners, and planned correc-
24 tive actions;

"(3) identifies costs associated with IBET units broken down by relevant categories designated at the Secretary's discretion;

"(4) identifies ways to support joint training for IBET stakeholder agencies and radio interoperability to allow for secure cross-border radio communications; and

"(5) identifies and assesses ways IBET, Border Tunnel Task Forces, Border Enforcement Security Task Forces, and the Integrated Cross-Border Maritime Law Enforcement Operation Program can better align operations, including interdiction and investigation activities.".

(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 439, as added by this title, the following new item:

"Sec. 440. Integrated Border Enforcement Teams.".

SEC. 431. NO BAN ON INFORMATION SHARING.

(a) IN GENERAL.—Subtitle C of title IV of the Homeland Security Act of 2002, as amended by this title, is further amended by adding at the end the following new section:

"SEC. 440A. ACCESS TO STATE, LOCAL, TRIBAL, AND TERRITORIAL INFORMATION.

"(a) AUTHORIZATION OF USE.—

"(1) IN GENERAL.—In the course of an investigation concerning a Federal crime within the jurisdiction of the Department, the Secretary may issue in writing and cause to be served a subpoena requiring the production of any biographical records, State-issued identification information, driving record information, vehicle registration information, or criminal history information of a specific individual from a State, local, Tribal, or territorial agency or department that the Secretary determines relevant to such investigation, or requiring testimony by the custodian of such materials to be produced concerning the production and authenticity of such materials.

"(2) CONTENTS.—A subpoena issued under paragraph (1) shall describe the information described in such paragraph required to be produced and prescribe a return date within a reasonable period of time within which such information can be assembled and made available.

"(3) PRODUCTION OF RECORDS.—The production of information under paragraph (1) may be required from any State, local, Tribal, or territorial agency or department in any State, or in any terri-

1 tory or other place subject to the jurisdiction of the
2 United States at any designated place of hearing.
3 ''(b) SERVICE.—
4 ''(1) IN GENERAL.—A subpoena issued under
5 this section may be served by any person designated
6 in the subpoena as the agent of service.
7 ''(2) SERVICE OF SUBPOENA.—
8 ''(A) STATE, LOCAL, TRIBAL, OR TERRI-
9 TORIAL AGENCIES AND DEPARTMENTS.—Serv-
10 ice of a subpoena may be made upon a State,
11 local, Tribal, or territorial agency or depart-
12 ment, by delivering the subpoena to an officer,
13 to a managing or general agent, or to any other
14 agent authorized by appointment or by law to
15 receive service of process.
16 ''(B) PROOF OF SERVICE.—The affidavit
17 of the person serving the subpoena entered by
18 that person on a true copy thereof shall be suf-
19 ficient proof of service.
20 ''(c) ENFORCEMENT.—
21 ''(1) IN GENERAL.—In the case of the contu-
22 macy by, or refusal to obey a subpoena issued to,
23 any State, local, Tribal, or territorial agency or de-
24 partment, the Secretary, in coordination with the
25 Attorney General, may invoke the aid of any court

of the United States within the jurisdiction of which the investigation described in subsection (a) is being conducted or within the jurisdiction that the subject of such investigation is located, to compel compliance with such subpoena.

"(2) ORDER.—A court of the United States described in paragraph (1) may issue an order requiring the subpoenaed State agency or department, in accordance with such subpoena, to appear, to produce records, or to give testimony relating to the matter under investigation. Any failure to obey the order of the court may be punished by the court as contempt thereof.

"(3) SERVICE OF PROCESS.—Any process under this subsection may be served in any judicial district in which the State, local, Tribal, or territorial agency or department may be found.

"(d) NONDISCLOSURE REQUIREMENT.—

"(1) IN GENERAL.—If the Secretary certifies that otherwise there may result a danger to the national security of the United States, no person may disclose to any other person that a subpoena was received or information was provided pursuant to this section, other than to—

"(A) those persons to whom such disclosure is necessary in order to comply with such subpoena;

"(B) an attorney to obtain legal advice with respect to testimony or the production of information in response to such subpoena; or

"(C) other persons as permitted by the Secretary.

"(2) NOTICE OF NONDISCLOSURE REQUIREMENT.—The subpoena, or an officer, employee, or agency of the United States in writing, shall notify the State, local, Tribal, or territorial agency or department to whom such subpoena is directed of the nondisclosure requirements under paragraph (1).

"(3) FURTHER APPLICABILITY OF NONDISCLOSURE REQUIREMENTS.—Any person who receives a disclosure under this subsection shall be subject to the same prohibitions on disclosure described in paragraph (1).

"(4) ENFORCEMENT OF NONDISCLOSURE REQUIREMENT.—Whoever knowingly violates paragraphs (1) or (3) shall be imprisoned for not more than one year, and if such violation is committed with the intent to obstruct an investigation or judi-

1 cial proceeding, shall be imprisoned for not more
2 than five years.
3 ''(5) TERMINATION OF NONDISCLOSURE RE-
4 QUIREMENT.—If the Secretary determines that a
5 nondisclosure requirement no longer is justified by a
6 danger to the national security of the United States,
7 an officer, employee, or agency of the United States
8 shall notify the relevant State, local, Tribal, or terri-
9 torial agency or department that the prohibition of
10 disclosure is no longer applicable.
11 ''(e) JUDICIAL REVIEW.—
12 ''(1) IN GENERAL.—At any time before the re-
13 turn date specified in a subpoena issued under this
14 section, the State, local, Tribal, or territorial agency
15 or department summoned may, in the United States
16 district court for the district in which such State,
17 local, Tribal, or territorial agency or department
18 does business or resides, petition for an order modi-
19 fying or setting aside such subpoena.
20 ''(2) MODIFICATION OF NONDISCLOSURE RE-
21 QUIREMENT.—Any court described in paragraph (1)
22 may modify or set aside a nondisclosure requirement
23 imposed under subsection (d) at the request of a
24 State, local, Tribal, or territorial agency or depart-
25 ment to whom a subpoena has been directed, unless

there is reason to believe that such nondisclosure requirement is justified because otherwise there may result a danger to the national security of the United States.

"(3) REVIEW OF GOVERNMENT SUBMISSIONS.—In all proceedings under this subsection, the court shall review the submission of the Federal Government, which may include classified information, ex parte and in camera.

"(f) IMMUNITY FROM CIVIL LIABILITY.—Any State, local, Tribal, or territorial agency or department, including officers, agents, and employees of a non-natural person, who in good faith produce the information requested in a subpoena, shall not be liable in any court of the United States to any customer or other person for such production, or for nondisclosure of such production to the customer or other person.

"(g) GUIDELINES.—The Secretary shall, by rule, establish such guidelines as are necessary to ensure the effective implementation of this section.

"(h) ANNUAL REPORTS.—The Secretary shall annually 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 (which may include a classified annex but

with the presumption of declassification) on the use of subpoenas under this subsection by the Secretary, which shall include a discussion of—

"(1) the number of and reason for the subpoenas issued under this section by the Secretary during the preceding year; and

"(2) a description of the outcome of each such subpoena.".

(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 440, as added by this title, the following new item:

"Sec. 440A. Access to State, local, Tribal, and territorial information.".

SEC. 432. BORDER SECURITY ADVISORY COMMITTEE.

(a) ESTABLISHMENT.—The Secretary of Homeland Security shall establish a Border Security Advisory Committee (referred to in this section as the "Advisory Committee").

(b) DUTIES.—

(1) IN GENERAL.—The Secretary of Homeland Security shall consult the Advisory Committee, as appropriate, on border security matters, including the following:

(A) Verifying security claims and the border security metrics established by the Department of Homeland Security under section 1092

of the National Defense Authorization Act for Fiscal Year 2017 (Public Law 114–328; 6 U.S.C. 223).

(B) Developing, refining, and implementing policies, programs, initiatives, rulemakings, and security directives pertaining to border security.

(2) RECOMMENDATIONS.—The Advisory Committee shall develop, at the request of the Secretary of Homeland Security, recommendations for improvements to border security and may provide, through the Secretary, recommendations to Congress.

(c) MEMBERSHIP.—

(1) COMPOSITION.—The Advisory Committee shall be composed of the following:

(A) Voting members appointed by the Secretary.

(B) Nonvoting members, serving in an advisory capacity, who shall be designated by—

(i) Customs and Border Protection;

(ii) Immigration and Customs Enforcement;

(iii) the Coast Guard; and

(iv) such other Federal department or agency as the Secretary considers appropriate.

(2) APPOINTMENT.—The Secretary of Homeland Security shall appoint voting members from among stakeholders including representatives from the following:

(A) Labor organizations representing federal law enforcement personnel with border security as their primary mission;

(B) Relevant Federal, State, local, and Tribal law enforcement, first responders, and security experts with at least five years of border security operations or research experience in a state that borders the northern, southern, or coastal borders of the United States.

(C) Former officials of the Department of Homeland Security with experience in border security.

(D) Other groups as the Secretary considers appropriate.

(3) CHAIRPERSON.—The Advisory Committee shall select a chairperson from among its voting members.

(4) TERM OF OFFICE.—

(A) IN GENERAL.—The term of each voting member of the Advisory Committee shall be 2 years, but a voting member may continue to serve until the Secretary of Homeland Security appoints a successor.

(B) REAPPOINTMENT.—A voting member of the Advisory Committee may be reappointed.

(C) REMOVAL.—The Secretary of Homeland Security may review the participation of a member of the Advisory Committee and remove such member for cause at any time.

(d) NONAPPLICABILITY OF FEDERAL ADVISORY COMMITTEE ACT.—The Federal Advisory Committee Act (5 U.S.C. App.) shall not apply to the Border Security Advisory Committee.

SEC. 433. BORDER TUNNEL DETECTION.

(a) IN GENERAL.—Subtitle B of title IV of the Homeland Security Act of 2002 (6 U.S.C. 211 et seq.), as amended by this title, is further amended by adding at the end the following new section:

"SEC. 420C. BORDER TUNNEL TASK FORCES.

''(a) ESTABLISHMENT.—There is established within the Department a program to be known as the Border Tunnel Task Force program (referred to in this section as 'BTTF').

1 "(b) PURPOSE.—The purpose of BTTF established
2 pursuant to subsection (a) is to enhance and integrate bor-
3 der security efforts by identifying, reducing, and remedi-
4 ating cross-border tunnel related threats by—
5 "(1) facilitating collaboration among Federal,
6 State, local, and Tribal law enforcement agencies to
7 execute coordinated activities; and
8 "(2) enhancing information-sharing, including
9 the dissemination of homeland security information,
10 among such agencies.
11 "(c) COMPOSITION AND ESTABLISHMENT OF BOR-
12 DER TUNNEL TASK FORCE UNITS.—
13 "(1) COMPOSITION.—BTTF units may be com-
14 prised of personnel from the following:
15 "(A) U.S. Customs and Border Protection,
16 led by the U.S. Border Patrol.
17 "(B) U.S. Immigration and Customs En-
18 forcement, led by Homeland Security Investiga-
19 tions.
20 "(C) Other Department components and
21 offices, as appropriate.
22 "(D) Other Federal, State, local, Tribal,
23 and foreign law enforcement agencies, as appro-
24 priate.

1 "(E) Other appropriate personnel at the
2 discretion of the Secretary.
3 "(2) ESTABLISHMENT OF UNITS.—The Sec-
4 retary is authorized to establish BTTF units in re-
5 gions in which the Secretary determines such units
6 can contribute to the Department's border security
7 efforts to identify, reduce, and remediate cross-bor-
8 der tunnel threats. When establishing a BTTF unit,
9 the Secretary shall apply risk-based criteria that
10 takes into consideration the following:
11 "(A) Whether the areas in which such
12 BTTF units would be established are signifi-
13 cantly impacted by cross-border tunnel threats.
14 "(B) The availability of Federal, State,
15 local, and Tribal law enforcement resources to
16 participate in such BTTF units.
17 "(C) Whether other similar joint cross-bor-
18 der tunnel detection initiatives already take
19 place within the region in which the BTTF unit
20 would be established.
21 "(d) DUPLICATION OF EFFORTS.—In determining
22 whether to establish a new BTTF unit or to expand an
23 existing BTTF unit in a given region, the Secretary shall
24 ensure that the BTTF unit under consideration does not

1 unnecessarily duplicate the efforts of other existing inter-
2 agency task forces or centers within such jurisdiction.
3 ''(e) OPERATION.—After determining the regions in
4 which to establish BTTF units under subsection (c)(2),
5 the Secretary may—
6 ''(1) direct the assignment of Federal personnel
7 to such BTTF units;
8 ''(2) take other actions to assist Federal, State,
9 local, and Tribal entities to participate in such
10 BTTF units, including providing financial assist-
11 ance, as appropriate, for operational, administrative,
12 and technological costs associated with such partici-
13 pation;
14 ''(3) direct the development of policy and guid-
15 ance necessary to identify, assess, and integrate the
16 available partner resources in relevant border sector
17 security assessments and resource planning docu-
18 ments;
19 ''(4) establish standard operating procedures,
20 targets, and performance measures for BTTF units;
21 and
22 ''(5) direct leadership of each BTTF unit to
23 monitor progress on such targets and performance
24 measures for each such unit.

1 "(f) COORDINATION.—The Secretary shall coordinate
2 BTTF activities with other similar border security and
3 antiterrorism programs within the Department that han-
4 dle matters relating to cross-border tunnel threat detec-
5 tion.

6 "(g) AUTHORIZATION OF TUNNEL REMEDIATION AC-
7 CESS.—Notwithstanding any other provision of law, U.S.
8 Customs and Border Protection shall have immediate ac-
9 cess to Federal land for the remediation of tunnels used
10 to facilitate illicit cross-border activities across the inter-
11 national borders of the United States.

12 "(h) REPORT.—Not later than 180 days after the
13 date on which BTTF is established and biannually there-
14 after for the following six years, the Secretary shall submit
15 to the Committee on Homeland Security of the House of
16 Representatives and the Committee on Homeland Security
17 and Governmental Affairs of the Senate a report that—

18 "(1) describes the effectiveness of BTTF in ful-
19 filling the purposes specified in subsection (b);

20 "(2) identifies challenges to the sustainment of
21 cross-border BTTF operations and planned correc-
22 tive actions;

23 "(3) identifies costs associated with BTTF
24 units broken down by relevant categories designated
25 at the Secretary's discretion;

"(4) identifies ways to support joint training for BTTF stakeholder agencies;

"(5) identifies and assesses ways BTTF, IBET, and Border Enforcement Security Task Forces can better align operations, including interdiction and investigation activities; and

"(6) identifies gaps in BTTF technological capability to detect cross-border tunnel threats.".

(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 420B, as added by this title, the following new item:

"Sec. 420C. Border Tunnel Task Forces.".

SEC. 434. SUBTERRANEAN OPERATIONS.

(a) IN GENERAL.—Subtitle B of title IV of the Homeland Security Act of 2002 (6 U.S.C. 211 et seq.), as amended by this title, is further amended by adding at the end the following new section:

"SEC. 420D. NATIONAL SUBTERRANEAN OPERATIONS PROGRAM.

"(a) ESTABLISHMENT.—There is established within U.S. Customs and Border Protection a program to known as the 'National Subterranean Operations Program' (referred to in this section as 'the program'). The program shall be headed by an Assistant Chief, who shall be appointed by the Chief of the U.S. Border Patrol.

1 ''(b) PURPOSE.—The purpose of the program is the
2 following:
3 ''(1) To apply risk-based criteria to interdict
4 and remediate illicit cross-border tunnels identified
5 by technology, intelligence leads, agency partners,
6 and relevant Federal entities as determined by the
7 Assistant Chief.
8 ''(2) To patrol and secure underground munic-
9 ipal infrastructure.
10 ''(c) AUTHORIZATION OF APPROPRIATIONS.—There
11 is authorized to be appropriated $4,000,000 for each of
12 fiscal years 2021 and 2022 to carry out this section.''.
13 (b) COUNTER TUNNEL OPERATIONS STRATEGIC
14 PLAN.—
15 (1) IN GENERAL.—Not later than 180 days
16 after the date of the enactment of this Act, the As-
17 sistant Chief of the National Subterranean Oper-
18 ations Program of U.S. Customs and Border Protec-
19 tion (established pursuant to section 420 of the
20 Homeland Security Act of 2002 (as added by sub-
21 section (a))) shall establish the following:
22 (A) Risk-based criteria to be used to
23 prioritize the interdiction and remediation of il-
24 licit cross-border tunnels identified by tech-
25 nology, intelligence leads, agency partners, and

other relevant Federal entities as determined by the Assistant Chief.

(B) Best practices for interdicting and remediating illicit cross-border tunnels.

(C) Processes, in coordination with Homeland Security Investigations and relevant Federal entities as determined by the Assistant Chief, to request and share relevant illicit cross-border tunnel location, operations, and technical information.

(D) Indicators of specific types of illicit cross-border tunnels found in each U.S. Border Patrol sector to be periodically disseminated to U.S. Border Patrol sector chiefs to educate field personnel.

(E) A counter illicit cross-border tunnel operations resource needs assessment that includes consideration of the following:

(i) Technology needs for conducting counter illicit cross-border tunnel operations.

(ii) Staffing needs, including the following::

(I) A position description for U.S. Border Patrol counter cross-border tunnel operations personnel.

(II) Specialized skills required of counter cross-border tunnel operations personnel.

(III) The number of full time employees needed to conduct illicit counter cross-border tunnel operations, disaggregated by U.S. Border Patrol sector.

(IV) Training requirements for identified staffing needs.

(2) REPORT TO CONGRESS.—Not later than one year after the date of enactment of this Act, the Commissioner of U.S. Customs and Border Protection 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 implementation of subsection (b).

(c) 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 420C, as added by this title, the following new item

"Sec. 420D. National Subterranean Operations Program.".

SEC. 435. BORDER ENFORCEMENT SECURITY TASK FORCE UPDATES.

(a) UPDATED PURPOSE.—Subsection (b) of section 432 of the Homeland Security Act of 2002 (6 U.S.C. 240) is amended—

(1) in paragraph (1), by striking ''and'' after the semicolon at the end;

(2) in paragraph (2), by striking the period at the end and inserting ''; and''; and

(3) by adding at the end the following new paragraph:

''(3) detecting, investigating, preventing, and responding to terrorism, transnational criminal organizations, and other violations of law related to border security.''.

(b) UPDATED CONSIDERATIONS FOR ESTABLISHMENT OF UNITS.—Paragraph (2) of section 432(c) of the Homeland Security Act of 2002 (6 U.S.C. 240(c)) is amended—

(1) in the matter preceding subparagraph (A)—

(A) in the first sentence, by striking ''jurisdictions'' and inserting ''regions'';

(B) by striking ''Before'' and inserting ''When''; and

(C) by striking ''shall consider'' and inserting ''shall apply risk-based criteria that takes into consideration'';

(2) in subparagraph (B), by inserting ''and'' after the semicolon at the end; and

(3) by striking subparagraphs (C) and (D) and inserting the following new subparagraph:

''(C) Whether, in accordance with paragraph (3), other joint cross-border initiatives already take place within the region in which the BEST unit would be established.''.

(c) UPDATED REPORT.—Subsection (e) of section 432 of the Homeland Security Act of 2002 (6 U.S.C. 240) is amended to read as follows:

''(e) REPORTS.—Not later than 180 days after the date of the enactment of this subsection and biannually thereafter for the following six years, 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 that—

''(1) describes the effectiveness of BEST units in fulfilling the purposes specified in subsection (b);

''(2) identifies challenges to the sustainment of cross-border BEST operations, including challenges

1 faced by international partners, and planned correc-
2 tive actions;
3 ''(3) identifies costs associated with BEST
4 units, broken down by relevant categories designated
5 at the Secretary's discretion;
6 ''(4) identifies ways to support joint training
7 for BEST stakeholder agencies;
8 ''(5) identifies and assesses ways BTTF under
9 section 420C, IBET units under section 440, and
10 BEST units can better align operations, including
11 interdiction and investigation activities; and
12 ''(6) identifies and assesses gaps in BEST tech-
13 nological capability to detect transnational criminal
14 organizations or terrorist threats.''.
15 (d) UPDATED REPORT.—Not later than 180 days
16 after the date of the enactment of this Act and biannually
17 thereafter for the following six years, the Secretary of
18 Homeland Security shall submit to the Committee on
19 Homeland Security of the House of Representatives and
20 the Committee on Homeland Security and Governmental
21 Affairs of the Senate the report reflected in subparagraph
22 (e).
23 (e) TECHNICAL AND CONFORMING AMENDMENTS.—
24 Section 432 of the Homeland Security Act of 2002 (6
25 U.S.C. 240) is amended—

(1) in subsection (c)—

(A) in paragraph (1)(D), by inserting a semicolon at the end; and

(B) in paragraph (3), by striking ''jurisdiction'' each place it appears and inserting ''region''; and

(2) in subsection (d), in the matter preceding paragraph (1), by striking ''jurisdictions'' and inserting ''regions''.

SEC. 436. EXTENSION OF PORT OF ENTRY DONATION AUTHORITY.

Subparagraph (A) of section 482(b)(4) of the Homeland Security Act of 2002 (6 U.S.C. 301a(b)(4)) is amended by striking ''4 years'' and inserting ''8 years''.

TITLE V—TRANSPORTATION SECURITY

SEC. 501. AUTHORIZATION OF APPROPRIATIONS FOR SALARIES, OPERATION, AND MAINTENANCE OF THE TRANSPORTATION SECURITY ADMINISTRATION.

Subsection (v) of section 114 of title 49, United States Code, is amended—

(1) in paragraph (2), by striking ''and'' after the semicolon at the end;

(2) in paragraph (3), by striking the period at the end and inserting "; and"; and

(3) by adding at the end the following new paragraph:

"(4) $8,076,294,000 for fiscal year 2022.".

SEC. 502. RETENTION OF SECURITY SERVICE FEE BY THE TRANSPORTATION SECURITY ADMINISTRATION.

(a) IN GENERAL.—Subsection (i) of section 44940 of title 49, United States Code, is repealed.

(b) CONFORMING AMENDMENT.—Paragraph (3) of section 44940(c) is amended by striking "Beginning on October 1, 2027, fees" and inserting "Fees".

SEC. 503. EMERGING AND FUTURE THREATS TASK FORCE.

(a) IN GENERAL.—Not later than 90 days after the date of the enactment of this Act, the Administrator of the Transportation Security Administration, in consultation with the Director of National Intelligence and the intelligence community (as such term is defined in section 3(4) of the National Security Act of 1947 (50 U.S.C. 3003(4))) and the heads of other Federal agencies, as determined appropriate by the Administrator, shall establish a task force to conduct an analysis of emerging and potential future threats to transportation security.

(b) MEMBERSHIP.—The task force established under subsection (a) shall be comprised of employees of the Department of Homeland Security who, in carrying out the analysis required under such subsection, shall consult with the Director of National Intelligence and the intelligence community and the heads of Federal agencies, as determined appropriate by the Administrator.

(c) DEADLINE.—Not later than 270 days after the Administrator establishes the task force under subsection (a), the task force shall submit to the Administrator the analysis required under such subsection.

(d) ELEMENTS.—The analysis required under subsection (a) shall include emerging and potential future threats posed by the following:

(1) Evolving tactics by terrorist organizations that may pose a catastrophic risk to an aviation or surface transportation entity.

(2) Explosive and explosive devices or attacks involving the use of explosives that may cause catastrophic damage to an aviation or surface transportation system.

(3) Chemical or biological agents being released in either aviation or surface transportation systems.

(4) Cyberthreat actors seeking to undermine confidence in transportation systems or cause service disruptions that jeopardize transportation security.

(5) Unmanned aerial systems with the capability of inflicting harm on transportation targets.

(6) Individuals or groups seeking to attack soft targets, public areas, or crowded spaces of transportation systems, including attacks against Transportation Security Administration employees and other security personnel.

(7) Foreign actors seeking to exploit vulnerabilities posed by the inconsistent or inadequate security screening protocols at last point of departure airports with direct flights to the United States.

(8) Information sharing challenges within the Federal Government and among partner governments.

(9) Information sharing challenges between the Administration or other relevant Federal agencies and transportation stakeholders, including air carriers, airport operators, surface transportation operators, and State and local law enforcement.

(10) Growth in passenger volume in both the aviation and surface transportation sectors.

(e) MITIGATION.—Not later than 120 days after the completion of the analysis required under subsection (a), the Administrator of the Transportation Security Administration shall develop, as appropriate, a threat mitigation strategy for each of the threats examined in such analysis, and—

(1) assign appropriate resources of the Administration to address such threats, based on calculated risk; or

(2) provide recommendations through the Department of Homeland Security to the appropriate Federal department or agency responsible for addressing such threats.

(f) STAKEHOLDER ENGAGEMENT.—When carrying out the analysis required under subsection (a), the Administrator of the Transportation Security Administration shall engage transportation stakeholders referred to in subsection (b)(9) and account for security concerns of transportation operators by—

(1) convening not fewer than three industry day events for such transportation stakeholders to hear from relevant public and private sector security partners and provide feedback on threats such transportation stakeholders identify as emerging;

(2) developing strategies to solicit feedback on a consistent basis from such transportation stakeholders across all modes of transportation and providing consistent responses to stakeholder concerns;

(3) improving the quality, timeliness, and relevancy of information sharing products disseminated by the Administration to such transportation stakeholders, including classified information sharing products;

(4) coordinating security incident response and communications drills, including tabletop exercises, to improve incident preparedness and response capabilities across transportation modes and among transportation systems;

(5) encouraging regular communication between Federal Security Directors, Field Intelligence Officers, Federal Air Marshal Special Agents in Charge, and such transportation stakeholders;

(6) establishing regular opportunities for senior Administration leadership to engage with such transportation stakeholders regarding changes in the threat environment and how the Administration can offer security support to address such changes; and

(7) briefing the Aviation Security Advisory Committee and the Surface Transportation Security

1 Advisory Committee on the efforts of the task force
2 established pursuant to subsection (a).
3 (g) BRIEFING TO CONGRESS.—The Administrator of
4 the Transportation Security Administration shall brief the
5 Committee on Homeland Security of the House of Rep-
6 resentatives and the Committee on Commerce, Science,
7 and Transportation of the Senate on the results of the
8 analysis required under subsection (a) and relevant miti-
9 gation strategies developed in accordance with subsection
10 (c).
11 (h) NON-APPLICABILITY OF FACA AND PRA.—The
12 Federal Advisory Committee Act (5 U.S.C. App.) and the
13 Paperwork Reduction Act (44 U.S.C. 3501 et seq.) shall
14 not apply to the task force established under subsection
15 (a).
16 **SEC. 504. COMPTROLLER GENERAL REVIEW.**
17 Not later than one year after the date of the enact-
18 ment of this Act, the Comptroller General of the United
19 States shall conduct a review of Department of Homeland
20 Security trusted traveler programs. Such review shall ex-
21 amine the following:
22 (1) The extent to which the Department of
23 Homeland Security tracks data and monitors trends
24 related to trusted traveler programs, including root
25 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. 505. ENROLLMENT REDRESS.

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 re-enrollment in such a program by such an individual.

SEC. 506. TRAINING REQUIRED.

(a) IN GENERAL.—Not later than 1 year after the date of the enactment of this Act, the Administrator of the Transportation Security Administration shall develop and implement training for frontline Administration personnel regarding the screening of pregnant women and families with young children at passenger screening checkpoints. Such training shall include the following:

(1) Information relating to concerns of pregnant women relating to the use of Advanced Imaging Technology and appropriate opt-out procedures and alternative screening procedures.

(2) Guidelines to assist pregnant women and families traveling with young children effectively and efficiently complete the screening process in a manner that is respectful and improves the overall functioning of the screening checkpoint.

(3) Communication and procedural guidelines for frontline Administration personnel to assist with passenger divestiture for pregnant women and families traveling with young children to improve the effectiveness and overall passenger experience at the screening checkpoint.

(b) COMMUNICATIONS STRATEGY.—In conjunction with the implementation of the training required under subsection (a), the Administrator of the Transportation Security Administration shall develop and implement a communications strategy for pregnant women and families traveling with young children to inform such women and families of the procedures and guidelines described in such subsection, including providing information to relevant passengers through social media, the Administration's public website, the Administration's customer service call center, and partnerships with aviation stakeholders, including air carriers and airport operators.

(c) PASSENGER SUPPORT SPECIALISTS.—In carrying out subsections (a) and (b), the Administrator of the Transportation Security Administration shall, to the extent possible, make available passenger support specialists, upon request, to pregnant women and families traveling with young children to assist with screening checkpoint information, concerns, and procedures.

(d) TSA FAMILY LANES FEASIBILITY ASSESSMENT.—Not later than 180 days after the date of the enactment of this Act, the Administrator of the Transportation Security Administration shall conduct a feasibility assessment to determine whether screening processes and the screening experience may be improved for travelers by

developing optional, dedicated screening lanes for families traveling with young children at airports where the checkpoint configuration would allow and where the overall functioning of the checkpoint would not be inhibited in terms of passenger throughput or security effectiveness.

(e) BRIEFING TO CONGRESS.—Not later than 30 days after the implementation of the training required under subsection (a), 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 progress regarding the implementation of this Act and improvements made to the screening process for pregnant women and families traveling with young children.

SEC. 507. IDENTITY AND TRAVEL DOCUMENT VERIFICATION.

Section 44901 of title 49, United States Code, is amended by adding at the end the following new subsection:

"(m) ESTABLISHMENT OF SCREENING SYSTEM FOR CERTAIN PERSONS.—Not later than December 31, 2020, the Administrator of the Transportation Security Administration shall, subject to the availability of appropriations, implement an identity and travel document verification

system designed to establish a secure, automated system at all airports for verifying identity and travel documents of persons seeking entry into the sterile area of an airport. Such system shall—

"(1) assess the need for security screening personnel to perform identity and travel document verification for such passengers, thereby assessing the overall number of such screening personnel;

"(2) reduce the average wait time of such passengers;

"(3) reduce overall operating expenses of the Administration;

"(4) be integrated with the Administration's watch list matching program; and

"(5) be integrated with other technologies to further facilitate risk-based passenger screening at checkpoints, to the extent practicable and consistent with security standards.".

SEC. 508. STANDARD OPERATING PROCEDURES AT AIRPORT CHECKPOINTS.

(a) STANDARDIZATION.—The Administrator of the Transportation Security Administration shall require, to the extent practicable, that standard operating procedures at airport checkpoints for passengers and carry-on bag-

gage are carried out in a uniform manner among similarly situated airports.

(b) REPORT TO CONGRESS.—Not later than 270 days after the date of the enactment of this Act, the Administrator of the Transportation Security Administration 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 on how standard operating procedures were made uniform in accordance with subsection (a).

(c) AUDITS.—Beginning one year after the date of the enactment of this Act, the Inspector General of the Department of Homeland Security shall conduct periodic audits of adherence to the standard operating procedures, as established by the Administrator of the Transportation Security Administration, under this section of screening personnel at large, medium, and small airports in diverse geographical areas.

SEC. 509. CANINE DETECTION RESEARCH AND DEVELOPMENT.

(a) IN GENERAL.—The Secretary of Homeland Security shall conduct an audit of all canine training programs of the Department of Homeland Security and convene a working group of representatives from all such programs to make recommendations on possible efficiencies that

could be gained by integrating training standards and facilities.

(b) CANINE STAFFING ALLOCATION MODEL.—The Administrator of the Transportation Security Administration shall develop a staffing allocation model for canines to determine the optimal number of passenger screening canines at airports in the United States.

(c) REPORT TO CONGRESS.—Not later than 180 days after the date of the enactment of this Act, the Secretary of Homeland Security 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 on the recommendations required by subsection (a).

(d) BRIEFING TO CONGRESS.—

(1) IN GENERAL.—Not later than 180 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 Homeland Security and Governmental Affairs and the Committee on Commerce, Science, and Transportation of the Senate on the state of explosives detection canine production and training in the United States.

(2) CONTENTS.—The briefing required under paragraph (1) shall include the following:

(A) An analysis of the steps the Transportation Security Administration may take to foster additional production of explosives detection canines in the United States by the private sector.

(B) Perspectives from current explosives detection canine industry stakeholders regarding the impact of the Administration's procurement model on business considerations.

(C) An analysis regarding whether the Administration effectively communicates canine training guidelines and testing methodology to the private sector.

(D) The extent to which physical capacity limitations at current Administration-operated sites hinder the operations of either the Administration or industry.

SEC. 510. SECURITY INCIDENT RESPONSE AT AIRPORTS AND SURFACE TRANSPORTATION HUBS.

The Gerardo Hernandez Airport Security Act of 2015 (Public Law 114–50; 49 U.S.C. 44903 note) is amended—

(1) in section 3—

(A) in subsection (b), in the matter preceding paragraph (1), by striking ''may'' each place it appears and inserting ''shall'';

(B) by redesignating subsection (c) as subsection (d); and

(C) by inserting after subsection (b) the following new subsection:

''(c) REVIEW.—The Administrator of the Transportation Security Administration shall review the active shooter response guidelines specified for Department of Homeland Security personnel under this section and make a recommendation to the Secretary of Homeland Security to modify such guidelines for personnel who are certified Federal law enforcement officials and for personnel who are uniformed but unarmed security officials.''; and

(2) in section 7—

(A) in subsection (b), in the matter preceding paragraph (1), by striking ''may'' each place it appears and inserting ''shall'';

(B) by redesignating subsections (c) and (d) as subsections (d) and (e), respectively; and

(C) by inserting after subsection (b) the following new subsection:

''(c) REVIEW.—The Administrator of the Transportation Security Administration shall review the active

shooter response guidelines specified for Department of Homeland Security personnel under this section and make a recommendation to the Secretary of Homeland Security to modify such guidelines for personnel who are certified Federal law enforcement officials and for personnel who are uniformed but unarmed security officials.''.

SEC. 511. ALTERNATE NEW SECURITY SCREENING PERSONNEL TRAINING PROGRAM COST AND FEASIBILITY STUDY.

Not later than 180 days after the date of the enactment of this Act, the Administrator of the Transportation Security Administration shall conduct a cost and feasibility study of developing a training program for security screening personnel that will provide such personnel with an equal level of training as is provided in the training program for new security screening personnel located at the Federal Law Enforcement Training Center in Glynco, Georgia, that could be conducted at or within 50 miles of such security screening personnel's duty station. Such study should examine the use of online seminar and training platforms for portions of the training curriculum that are conducive to such an outcome.

SEC. 512. PROHIBITION OF ADVANCE NOTICE OF COVERT TESTING TO SECURITY SCREENERS.

Section 44935 of title 49, United States Code, is amended by adding at the end the following new subsection:

"(m) PROHIBITION OF ADVANCE NOTICE TO SECURITY SCREENERS OF COVERT TESTING AND EVALUATION.—

"(1) IN GENERAL.—The Administrator of the Transportation Security Administration shall ensure, to the greatest extent practicable, that information concerning a covert test of a transportation security system to be conducted by a covert testing office, the Inspector General of the Department of Homeland Security, or the Government Accountability Office is not provided to any individual involved in such test prior to the completion of such test.

"(2) EXCEPTIONS.—Notwithstanding paragraph (1)—

"(A) an authorized individual involved in a covert test of a transportation security system may provide information concerning such covert test to—

"(i) employees, officers, and contractors of the Federal Government (including military personnel);

1 ''(ii) employees and officers of State
2 and local governments; and
3 ''(iii) law enforcement officials who
4 are authorized to receive or directed to be
5 provided such information by the Adminis-
6 trator of the Transportation Security Ad-
7 ministration, the Inspector General of the
8 Department of Homeland Security, or the
9 Comptroller General of the United States,
10 as the case may be; and
11 ''(B) for the purpose of ensuring the secu-
12 rity of any individual in the vicinity of a site at
13 which a covert test of a transportation security
14 system is being conducted, an individual con-
15 ducting such test may disclose his or her status
16 as an individual conducting such test to any ap-
17 propriate individual if a security screener or
18 other individual who is not a covered employee
19 identifies the individual conducting such test as
20 a potential threat.
21 ''(3) SPECIAL RULES FOR TSA.—
22 ''(A) MONITORING AND SECURITY OF
23 TESTING PERSONNEL.—The head of each covert
24 testing office shall ensure that a person or
25 group of persons conducting a covert test of a

transportation security system for a covert testing office is accompanied at the site of such test by a cover team composed of one or more employees of such covert testing office for the purpose of monitoring such test and confirming the identity of personnel involved in such test under subparagraph (B).

''(B) RESPONSIBILITY OF COVER TEAM.—Under this paragraph, a cover team for a covert test of a transportation security system shall—

''(i) monitor such test; and

''(ii) for the purpose of ensuring the security of any individual in the vicinity of a site at which such test is being conducted, confirm, notwithstanding paragraph (1), the identity of any individual conducting such test to any appropriate individual if a security screener or other individual who is not a covered employee identifies the individual conducting such test as a potential threat.

''(C) AVIATION SCREENING.—Notwithstanding subparagraph (A), the Transportation Security Administration is not required to have a cover team present during a test of the

1 screening of persons, carry-on items, or checked
2 baggage at an aviation security checkpoint at or
3 serving an airport if such test is—
4 ''(i) approved, in coordination with
5 the designated security official for the air-
6 port operator by the Federal Security Di-
7 rector for such airport; and
8 ''(ii) carried out under an aviation
9 screening assessment program of the De-
10 partment of Homeland Security.
11 ''(D) USE OF OTHER PERSONNEL.—The
12 Transportation Security Administration may
13 use employees, officers, and contractors of the
14 Federal Government (including military per-
15 sonnel) and employees and officers of State and
16 local governments or any personnel authorized
17 by the Federal Security Director to conduct
18 covert tests.
19 ''(4) DEFINITIONS.—In this subsection, the fol-
20 lowing definitions apply:
21 ''(A) APPROPRIATE INDIVIDUAL.—The
22 term 'appropriate individual', as used with re-
23 spect to—
24 ''(i) a covert test under paragraph
25 (2)(B) of a transportation security system,

means any individual who the individual conducting such test determines needs to know his or her status as an individual conducting such test; or

"(ii) a covert test under paragraph (3)(B)(i), means any individual who the cover team monitoring such test determines needs to know the identity of such cover team.

"(B) COVERED EMPLOYEE.—The term 'covered employee' means any individual who receives notice of a covert test before the completion of a test under paragraph (2)(B).

"(C) COVERT TEST.—

"(i) IN GENERAL.—The term 'covert test' means an exercise or activity conducted by a covert testing office, the Inspector General of the Department of Homeland Security, or the Government Accountability Office to intentionally test, compromise, or circumvent transportation security systems to identify vulnerabilities in such systems.

"(ii) LIMITATION.—Notwithstanding clause (i), the term 'covert test' does not

mean an exercise or activity by an employee or contractor of the Transportation Security Administration to test or assess compliance with relevant regulations.

''(D) COVERT TESTING OFFICE.—The term 'covert testing office' means any office of the Transportation Security Administration designated by the Administrator of the Transportation Security Administration to conduct covert tests of transportation security systems.

''(E) EMPLOYEE OF A COVERT TESTING OFFICE.—The term 'employee of a covert testing office' means an individual who is an employee of a covert testing office or a contractor or an employee of a contractor of a covert testing office.''.

SEC. 513. EXPLOSIVE DETECTION TECHNOLOGY.

The Secretary of Homeland Security shall prioritize the research and facilitation of next generation technologies to detect explosives in the Nation's surface transportation systems.

SEC. 514. RECURRENT VETTING FOR SURFACE TRANSPORTATION CREDENTIAL-HOLDERS.

Section 70105 of title 46, United States Code, is amended by adding at the end the following new subsection:

"(r) RECURRENT VETTING.—

"(1) IN GENERAL.—Not later than 180 days after the date of the enactment of this subsection, the Secretary shall develop and implement a plan to utilize the Federal Bureau of Investigation's Rap Back Service in order to establish recurrent vetting capabilities for individuals holding valid transportation security cards under this section.

"(2) EXEMPTION.—Individuals holding valid transportation security cards under this section who are subject to recurrent vetting under the plan to utilize the Rap Back Service referred to in paragraph (1) shall be exempt from any recurrent determinations or background checks under this section to which such individuals would otherwise be subject every five years in the absence of such utilization.".

SEC. 515. BIOMETRICS FOR TSA PRECHECK.

(a) IN GENERAL.—Not later than September 30, 2023, the Administrator of the Transportation Security Administration shall begin the utilization of biometrics to verify the identity of travelers enrolled in the Administra-

tion's trusted traveler program, known as TSA PreCheck, at security screening checkpoints in a manner which—

(1) protects the privacy and civil liberties of the traveling public;

(2) improves the security and functionality of the security screening checkpoint;

(3) leverages, to the extent practicable, existing biometric repositories of the Department of Homeland Security; and

(4) utilizes best available biometric technology and algorithms to reduce instances of misidentification.

(b) WORKING GROUP ESTABLISHED.—Not later than 30 days after the date of the enactment of this Act, the Administrator of the Transportation Security Administration shall establish a working group comprised of relevant transportation security stakeholders and any personnel determined necessary by the Administrator to inform and make recommendations for the successful implementation of a biometrics identity process.

(c) REPORT TO CONGRESS.—Not later than one year after the date of the enactment of this Act and annually thereafter through 2023, the Administrator of the Transportation Security Administration shall report to the Committee on Homeland Security of the House of Representa-

tives and the Committee on Commerce, Space, and Transportation of the Senate on the status of the Administration's biometrics program.

SEC. 516. SECURE FLIGHT PROGRAM.

(a) IN GENERAL.—Not later than 180 days after the date of the enactment of this Act, the Administrator of the Transportation Security Administration shall ensure that security screening checkpoints have real-time connectivity to the Administration's Secure Flight vetting system.

(b) SECURE FLIGHT REVIEW.—Not later than 1 year after the date of the enactment of this Act, the Administrator of the Transportation Security Administration shall develop and implement a plan to improve the capabilities of the Administration's Secure Flight program, including—

(1) improving coordination between Secure Flight and air carriers;

(2) reducing screening errors resulting from inaccurate or delayed Secure Flight data; and

(3) identifying additional resources needed to upgrade information technology systems of Secure Flight.

SEC. 517. KNOWN CREW MEMBER PROGRAM.

(a) IN GENERAL.—Not later than 180 days after the enactment of this Act, the Administrator of the Transportation Security Administration shall implement new security standards for the Administration's Known Crew Member program, including—

(1) updated standards for verifying crew identity at Known Crew Member-enabled checkpoints; and

(2) cybersecurity standards for the Known Crew Member program.

(b) COORDINATION.—In carrying out the requirements of subsection (a), the Administrator of the Transportation Security Administration shall coordinate with relevant transportation security stakeholders, including air carriers and labor organizations representing pilots and flight attendants.

SEC. 518. SCREENING PARTNERSHIP PROGRAM.

(a) IN GENERAL.—The Administrator of the Transportation Security Administration shall promote and encourage airport participation in the Administration's Screening Partnership Program.

(b) BLUE RIBBON PANEL.—Not later than 90 days after the date of the enactment of this Act, the Administrator of the Transportation Security Administration shall convene a Blue Ribbon Panel to examine ways in which

the Screening Partnership Program can be improved, including—

(1) allowing greater input for airport terminal owners and operators into selecting a screening vendor;

(2) reducing costs to the taxpayer by expanding the Screening Partnership Program; and

(3) examining security screening programs of foreign partners to outline best practices for public private partnership for passenger screening.

SEC. 519. HEADQUARTERS EFFICIENCY.

Not later than 1 year after the date of the enactment of this Act, the Administrator of the Transportation Security Administration shall seek to reduce by 50 percent administrative support contract costs for headquarters personnel.

SEC. 520. REPEAL OF REGULATIONS.

Sections 1408, 1517, and 1534 of the Implementing Recommendations of the 9/11 Commission Act of 2007 are repealed.

SEC. 521. SENSITIVE SECURITY INFORMATION.

(a) 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—

(1) ensure clear and consistent designation of ''Sensitive Security Information'', including reasonable security justifications for so designating documents as such;

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

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

(4) 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

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

(b) 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 subsection (a)(4) that regularly are granted access to Sensitive Security Information to raise awareness

of the TSA's policies and guidelines governing the classification and use of Sensitive Security Information.

SEC. 522. INTERNATIONAL AVIATION SECURITY.

(a) 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—

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

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

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

(4) 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

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

(b) 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, Space, and Transportation of the Senate on the guidelines described in this section.

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

SEC. 523. OFFICE OF INSPECTION ACCOUNTABILITY.

(a) IN GENERAL.—The Administrator of the Transportation Security Administration shall strengthen internal controls related to documentation accuracy of the Office of Inspection of the Administration by developing and implementing—

(1) updates to criminal investigators' performance plans to reflect timely and accurate timesheet submission;

(2) guidance and expectation for supervisory biweekly timesheet review; and

(3) a formal plan for reviewing user access, not less than annually, to ensure appropriate system access and permission levels.

(b) INFORMATION SYSTEMS.—The Administrator of the Transportation Security Administration shall work to establish systems to assist the Office of Inspection of the Administration with timesheet submission and approval processes and improve data transfer and communication between the timekeeping system and the Case Management System.

(c) PREMIUM PAY ELIGIBILITY.—The Administrator of the Transportation Security Administration shall develop, formalize, and implement processes to ensure compliance with relevant policies requiring criminal investigators and supervisors annually complete documentation certifying availability for Law Enforcement Availability Pay.

(d) RESOURCE ALLOCATION.—The Administrator of the Transportation Security Administration shall develop and implement guidance to ensure proper review of annual

calculations for resource allocation within the Office of Inspection of the Administration.

SEC. 524. CHECKPOINTS OF THE FUTURE.

(a) IN GENERAL.—The Administrator of the Transportation Security Administration shall develop passenger self-screening solutions for PreCheck passengers in a manner which—

(1) does not reduce the overall security posture of the checkpoint; and

(2) improves the efficiency and overall effectiveness of the checkpoint.

(b) REPORT TO CONGRESS.—Not later than 180 days after the enactment of this Act and annually thereafter for 5 years, the Administrator of the Transportation Security Administration shall submit to the Committee on Homeland Security of the House of Representatives and the Committee on Commerce, Space, and Transportation of the Senate a report on the status of the requirements described in subsection (a).

SEC. 525. AIR CARGO SECURITY.

Not later than one year after the date of the enactment of this Act the Inspector General for the Department of Homeland Security shall conduct an audit of the Air Cargo Division of the Transportation Security Administration of the Department. This audit shall include—

(1) a review of resource and staffing allocations for the Air Cargo Division;

(2) an examination of how the Air Cargo Division's effectiveness in managing the Certified Cargo Screening Program and Known Shipper Program; and

(3) how effectively the Air Cargo Division works collaboratively with U.S. Customs and Border Protection to target high-risk cargo.

SEC. 526. CHILDCARE.

(a) IN GENERAL.—Not later than 30 days after the date of the enactment of this Act, the Administrator of the Transportation Security Administration shall convene a working group comprised of personnel determined appropriate by the Administrator to develop—

(1) recommendations for establishing childcare facilities for employees at the Administration's headquarters facility;

(2) recommendations for establishing a facility or otherwise assisting with childcare options for employees at airports; and

(3) options for the Administration to improve flexibility for employees with children in need of care.

(b) REPORT TO CONGRESS.—Not later than 1 year after the date of the enactment of this Act, the Administrator of the Transportation Security Administration shall submit to the Committee on Homeland Security of the House of Representatives and the Committee on Commerce, Space, and Technology of the Senate a report on the recommendations and findings of the working group established in subsection (a).

SEC. 527. PASSENGERS WITH PHYSICAL OR COGNITIVE DISABILITIES.

Not later than one year after the date of the enactment of this Act, the Administrator of the Transportation Security Administration shall convene an event at each airport at which the Administration conducts security screening to increase awareness, understanding of screening protocols, and efficiency of the passenger screening experience for passengers with physical or cognitive disabilities.

SEC. 528. TSA HUMAN CAPITAL STRATEGIC PLAN.

(a) HUMAN CAPITAL STRATEGIC PLAN DEFINED.—In this section, the term ''human capital strategic plan'' means a plan to evaluate and implement strategies for the Transportation Security Administration's selecting, developing, training, and managing a high-quality, productive workforce in accordance with merit system principles de-

1 scribed in section 250.202 of title 5, Code of Federal Reg-
2 ulations (relating to primary duties of an agency's Chief
3 Human Capital Officer).

4 (b) TRANSPORTATION SECURITY STRATEGIC PLAN-
5 NING.—Paragraph (3) of section 114(s) of title 49, United
6 States Code, is amended by adding at the end the fol-
7 lowing new subparagraph:

8 "(J) A Human Capital Strategic Plan that
9 considers the recommendations contained in the
10 Findings and Recommendations of the 2019
11 Blue Ribbon Panel for the Transportation Se-
12 curity Administration on Human Capital Serv-
13 ice Delivery Evaluation or any successor docu-
14 ment. Priority for consideration shall be given
15 to the recommendations from the Panel that
16 address the use of scheduling and timekeeping
17 tools, the review and updating of recruiting ma-
18 terials, the development of standardized job de-
19 scriptions, the examination of Transportation
20 Security Administration employer branding and
21 recruiting methods, the development of a proc-
22 ess to receive feedback on Human Capital func-
23 tions, and the improvement of leadership devel-
24 opment and feedback mechanisms.".

SEC. 529. SCREENING TECHNOLOGY DEPLOYMENT.

(a) IN GENERAL.—Not later than 180 days after the date of the enactment of this Act, the Administrator of the Transportation Security Administration shall implement a policy to produce deployment plans for screening technology. Such plans should—

(1) include airport risk assessments and all relevant risk factors;

(2) consider relative airport risk when determining deployment order;

(3) provide rationale for deployment decisions, including any specific risk factors considered;

(4) include a strategy for deployment to small and medium airports to ensure consistency of security operations across airports of all sizes; and

(5) include procurement strategy for each screening technology to be deployed.

(b) CONTINUOUS EVALUATION OF DEPLOYED EQUIPMENT.—Not later than 180 days after the date of the enactment of this Act, the Administrator of the Transportation Security Administration shall develop a strategy for continuous evaluation of deployed screening technology. In developing such strategy, the Administrator shall consider the following:

(1) The effectiveness of screening during the lifespan of screening technology.

(2) How maintenance contracts for procured screening technology can support the Administration's efforts to ensure continued effectiveness after deployment of such technology.

(3) Periodic testing for the effectiveness of deployed screening technology based on relative risk.

(c) AUDITS.—Beginning one year after the date of the enactment of this Act, the Inspector General of the Department of Homeland Security shall conduct an audit of the Transportation Security Administration's efforts to develop and implement deployment plans for screening technology. Such audit shall determine if—

(1) the Administration has effectively produced risk-based deployment plans for screening technologies;

(2) the screening technology deployment adhered to deployment plans; and

(3) the deployment rate of screening technologies by type across airport size and geographical areas.

(d) BRIEFING TO CONGRESS.—Not later than 270 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 Com-

merce, Science, and Transportation of the Senate on the requirements described in this section.

SEC. 530. REVIEW OF AVIATION SECURITY STAKEHOLDER ACCESS TO HOMELAND SECURITY INFORMATION NETWORK.

The Secretary of Homeland Security, in coordination with the Under Secretary for Intelligence and Analysis of the Department of Homeland Security, shall review access to the Homeland Security Information Network to determine if access by aviation security stakeholders in addition to such stakeholders who already as of the date of the enactment of this Act already have such access would benefit aviation security.

SEC. 531. AIRPORT PUBLIC AREA SECURITY ENHANCEMENT.

(a) AIRPORT PUBLIC AREA SECURITY WORKING GROUP ENGAGEMENT PLAN.—

(1) IN GENERAL.—Not later than one year after the date of the enactment of this Act, the Administrator of the Transportation Security Administration (TSA) shall implement a plan to enhance TSA engagement with the public area security working group established in accordance with section 1931 of the FAA Reauthorization Act of 2018 (49 U.S.C. 114 note; Public Law 115–254). Such plan

shall include descriptions of roles and responsibilities for group members, mechanisms for collaboration, and determinations regarding the frequency of working group meetings.

(2) BRIEFING TO CONGRESS.—Not later than 30 days after implementation of the plan required under paragraph (1) is complete, the Administrator shall brief the appropriate committees of Congress on the details of such plan.

(b) SURVEY OF AIRPORT PUBLIC AREA SECURITY EFFORTS.—

(1) IN GENERAL.—Not later than 180 days after the date of the enactment of this Act, the Administrator shall begin conducting a survey of public and private stakeholders responsible for securing airport public areas to assess the following:

(A) The number of airport operations centers.

(B) The activities in which such airport operations centers regularly engage.

(C) The stakeholders involved in such airport operations centers, including information relating to staffing and participation of such stakeholders.

(D) Availability of resources for such airport operations centers.

(E) Technology used to monitor and secure airport public areas.

(F) Interoperability or other challenges associated with communication or other information technology systems supporting such airport operations centers.

(G) Policies and best practices used to provide situational awareness and coordinate airport public area security efforts.

(2) BRIEFING TO CONGRESS.—Not later than 30 days after completion of the survey required under subsection (1), the Administrator shall brief the appropriate committees of Congress a report on the findings of such survey.

(c) TSA SUPPORT OF AIRPORT OPERATIONS CENTERS.—

(1) IN GENERAL.—Not later than 90 days after the briefing required under subsection (b)(2) and not less frequently than once every five years thereafter, the Administrator shall develop and update, respectively, a strategy for Administration engagement with airport operations centers. Such strategy shall—

(A) include specific goals and objectives for the support of such airport operations centers managed by public and private stakeholders responsible for securing airport public areas; and

(B) detail means of support—

(i) to direct deployment of Administration personnel to such airport operations centers;

(ii) to provide to such stakeholders, as appropriate, access to Department unclassified or classified information sharing systems, including the Homeland Security Information Network and Homeland Security Data Network; and

(iii) for any activities determined appropriate by the Administrator.

(2) BRIEFING TO CONGRESS.—Not later than 30 days after the strategy under subsection (1) is complete, the Administrator shall brief the appropriate committees of Congress on the implementation of such strategy.

(d) DEFINITIONS.—In this section:

(1) ADMINISTRATION; TSA.—The terms ''Administration'' and ''TSA'' mean the Transportation Security Administration.

(2) ADMINISTRATOR.—The term ''Administrator'' means the Administrator of the Administration.

(3) APPROPRIATE COMMITTEES OF CONGRESS.—The term ''appropriate committees of Congress'' means the Committee on Homeland Security of the House of Representatives and the Committee on Commerce, Science, and Transportation of the Senate.

(4) DEPARTMENT.—The term ''Department'' means the Department of Homeland Security.

(5) OPERATIONS CENTER.—The term ''operations center'' means a integrated and unified operation center established at a transportation facility based on the framework made available to public and private stakeholders pursuant to section 1987 of the FAA Reauthorization Act of 2018 (49 U.S.C. 114 note; Public Law 115–254).

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

TITLE VI—EMERGENCY PREPAREDNESS, RESPONSE, AND RECOVERY

Subtitle A—Grants, Training, Exercises, and Coordination

SEC. 601. URBAN AREA SECURITY INITIATIVE.

Section 2003 of the Homeland Security Act of 2002 (6 U.S.C. 604) is amended—

(1) in subsection (b)(2)(A), in the matter preceding clause (i), by inserting ", using the most up-to-date data available," after "assessment";

(2) in subsection (d)(2), by amending subparagraph (B) to read as follows:

"(B) FUNDS RETAINED.—To ensure transparency and avoid duplication, a State shall provide each relevant high-risk urban area with a detailed accounting of the items, services, or activities on which any funds retained by the State under subparagraph (A) are to be expended. Such accounting shall be provided not later than 90 days after the date of which such funds are retained."; and

(3) by striking subsection (e) and inserting the following new subsections:

"(e) THREAT AND HAZARD IDENTIFICATION RISK ASSESSMENT AND CAPABILITY ASSESSMENT.—As a condition of receiving a grant under this section, each high-risk urban area shall submit to the Administrator a threat and hazard identification and risk assessment and capability assessment—

"(1) at such time and in such form as is required by the Administrator; and

"(2) consistent with the Federal Emergency Management Agency's Comprehensive Preparedness Guide 201, Second Edition, or such successor document or guidance as is issued by the Administrator.

"(f) PERIOD OF PERFORMANCE.—The Administrator shall make funds provided under this section available for use by a recipient of a grant for a period of not less than 36 months.

"(g) AUTHORIZATION OF APPROPRIATIONS.—There is authorized to be appropriated for grants under this section $800,000,000 for each of fiscal years 2021 through 2022.".

SEC. 602. STATE HOMELAND SECURITY GRANT PROGRAM.

Section 2004 of the Homeland Security Act of 2002 (6 U.S.C. 605) is amended by striking subsection (f) and inserting the following new subsections:

1 "(f) THREAT AND HAZARD IDENTIFICATION AND
2 RISK ASSESSMENT AND CAPABILITY ASSESSMENT.—
3 "(1) IN GENERAL.—As a condition of receiving
4 a grant under this section, each State shall submit
5 to the Administrator a threat and hazard identifica-
6 tion and risk assessment and capability assess-
7 ment—
8 "(A) at such time and in such form as is
9 required by the Administrator; and
10 "(B) consistent with the Federal Emer-
11 gency Management Agency's Comprehensive
12 Preparedness Guide 201, Second Edition, or
13 such successor document or guidance as is
14 issued by the Administrator.
15 "(2) COLLABORATION.—In developing the
16 threat and hazard identification and risk assessment
17 under paragraph (1), a State shall solicit input from
18 local and Tribal governments, including first re-
19 sponders, and, as appropriate, nongovernmental and
20 private sector stakeholders.
21 "(3) FIRST RESPONDERS DEFINED.—In this
22 subsection, the term 'first responders' includes rep-
23 resentatives of local governmental and nongovern-
24 mental fire, law enforcement, emergency manage-
25 ment, and emergency medical personnel.

"(g) PERIOD OF PERFORMANCE.—The Administrator shall make funds provided under this section available for use by a recipient of a grant for a period of not less than 36 months.

"(h) AUTHORIZATION OF APPROPRIATIONS.—There is authorized to be appropriated for grants under this section $600,000,000 for each of fiscal years 2021 through 2022.".

SEC. 603. GRANTS TO DIRECTLY ELIGIBLE TRIBES.

Section 2005 of the Homeland Security Act of 2002 (6 U.S.C. 606) is amended by—

(1) redesignating subsections (h) through (k) as subsections (i) through (l), respectively; and

(2) inserting after subsection (g) the following new subsection:

"(h) PERIOD OF PERFORMANCE.—The Secretary shall make funds provided under this section available for use by a recipient of a grant for a period of not less than 36 months.".

SEC. 604. LAW ENFORCEMENT TERRORISM PREVENTION.

(a) LAW ENFORCEMENT TERRORISM PREVENTION PROGRAM.—Subsection (a) of section 2006 of the Homeland Security Act of 2002 (6 U.S.C. 607) is amended—

(1) in paragraph (1)—

(A) by inserting ''States and high-risk urban areas expend'' after ''that''; and

(B) by striking ''is used'';

(2) in paragraph (2), by amending subparagraph (I) to read as follows:

''(I) activities as determined appropriate by the Administrator, in coordination with the Assistant Secretary for State and Local Law Enforcement within the Office of Partnership and Engagement of the Department, through outreach to relevant stakeholder organizations; and''; and

(3) by adding at the end the following new paragraph:

''(4) ANNUAL REPORT.—The Administrator, in coordination with the Assistant Secretary for State and Local Law Enforcement, shall report annually from fiscal year 2021 through fiscal year 2022 on the use of grants under sections 2003 and 2004 for law enforcement terrorism prevention activities authorized under this section, including the percentage and dollar amount of funds used for such activities and the types of projects funded.''.

(b) OFFICE FOR STATE AND LOCAL LAW ENFORCEMENT.—Subsection (b) section 2006 of the Homeland Security Act of 2002 (6 U.S.C. 607) is amended—

(1) in paragraph (1), by striking ''Policy Directorate'' and inserting ''Office of Partnership and Engagement''

(2) in paragraph (4)—

(A) in subparagraph (B), by inserting '', including through consultation with such agencies regarding Department programs that may impact such agencies'' before the semicolon at the end; and

(B) in subparagraph (D), by striking ''ensure'' and inserting ''certify''.

SEC. 605. PRIORITIZATION.

(a) IN GENERAL.—Subsection (a) of section 2007 of the Homeland Security Act of 2002 (6 U.S.C. 608) is amended—

(1) in paragraph (1)—

(A) by amending subparagraph (A) to read as follows:

''(A) its population, including consideration of domestic and international tourists, commuters, and military populations, including

military populations residing in communities outside military installations;'';

(B) in subparagraph (E), by inserting '', including threat information from other relevant Federal agencies and field offices, as appropriate'' before the semicolon at the end; and

(C) in subparagraph (I), by striking ''target'' and inserting ''core''; and

(2) in paragraph (2), by striking ''target'' and inserting ''core''.

(b) REVIEW.—Not later than 90 days after the date of the enactment of this Act, the Secretary of Homeland Security, through the Administrator of the Federal Emergency Management Agency, shall review and report to the Committee on Homeland Security and the Committee on Appropriations of the House of Representatives and the Committee on Homeland Security and Governmental Affairs and the Committee on Appropriations of the Senate on the risk formula and methodology used to award grants under sections 2003 and 2004 of the Homeland Security Act of 2002 (6 U.S.C. 604 and 605), including a discussion of any necessary changes to such formula to ensure grant awards are appropriately based on risk.

(c) COMPTROLLER GENERAL REVIEW.—Not later than 180 days after the date of enactment of this Act,

the Comptroller General of the United States shall review and assess the risk formula and methodology used to award grants under sections 2003 and 2004 of the Homeland Security Act of 2002, including—

(1) the process utilized by the Department of Homeland Security to gather threat information for each potential State and high-risk urban area;

(2) the extent to which such risk formula and methodology considers the factors specified in section 2007 of the Homeland Security Act of 2002 (6 U.S.C. 608), in particular—

(A) the extent to which the jurisdiction has unmet core capabilities due to resource constraints;

(B) the degree to which a jurisdiction has been able to address capability gaps with previous grant awards; and

(C) in the case of a high-risk urban area, the extent to which such high-risk urban area includes—

(i) incorporated municipalities, counties, parishes, and Indian Tribes within the relevant eligible metropolitan area the inclusion of which will enhance regional efforts to prevent, prepare for, protect

against, and respond to acts of terrorism; and

(ii) other local and Tribal governments in the surrounding area that are likely to be called upon to respond to acts of terrorism within the high-risk urban area; and

(3) how grant award amounts are determined.

SEC. 606. ALLOWABLE USES.

Section 2008 of the Homeland Security Act of 2002 (6 U.S.C. 609) is amended—

(1) in subsection (a)—

(A) in the matter preceding paragraph (1), by striking ''target'' and inserting ''core'';

(B) by redesignating paragraphs (6) through (14) as paragraphs (8) through (16), respectively;

(C) in paragraph (5), by inserting before the semicolon at the end the following: '', provided such purchases align with the Statewide Communication Interoperability Plan and are coordinated with the Statewide Interoperability Coordinator or Statewide interoperability governance body of the State of the recipient''; and

(D) by inserting after paragraph (5) the following new paragraphs:

''(6) enhancing medical preparedness, medical surge capacity, and mass prophylaxis capabilities, including the development and maintenance of an initial pharmaceutical stockpile, including medical kits and diagnostics sufficient to protect first responders, their families, immediate victims, and vulnerable populations from a chemical or biological event;

''(7) enhancing cybersecurity, including preparing for and responding to cybersecurity risks and incidents (as such terms are defined in section 227) and developing statewide cyber threat information analysis and dissemination activities;'';

(E) in paragraph (8), as so redesignated, by striking ''Homeland Security Advisory System'' and inserting ''National Terrorism Advisory System''; and

(F) in paragraph (14), as so redesignated, by striking ''3'' and inserting ''5'';

(2) in subsection (b)—

(A) in paragraph (3)(B), by striking ''(a)(10)'' and inserting ''(a)(12)''; and

(B) in paragraph (4)(B)(i), by striking ''target'' and inserting ''core''; and

(3) in subsection (c), by striking ''target'' and ''core''.

SEC. 607. MEMORANDA OF UNDERSTANDING.

(a) IN GENERAL.—Subtitle B of title XX of the Homeland Security Act of 2002 (6 U.S.C. 611 et seq.) is amended by adding at the end the following new section:

''SEC. 2024. MEMORANDA OF UNDERSTANDING WITH DEPARTMENTAL COMPONENTS AND OFFICES.

''The Administrator shall enter into memoranda of understanding with the heads of the following departmental components and offices delineating the roles and responsibilities of such components and offices regarding the policy and guidance for grants under section 1406 of the Implementing Recommendations of the 9/11 Commission Act of 2007 (6 U.S.C. 1135), sections 2003 and 2004 of this Act, and section 70107 of title 46, United States Code, as appropriate:

''(1) The Commissioner of U.S. Customs and Border Protection.

''(2) The Administrator of the Transportation Security Administration.

''(3) The Commandant of the Coast Guard.

''(4) The Under Secretary for Intelligence and Analysis.

"(5) The Director of the Office of Emergency Communications.

"(6) The Assistant Secretary for State and Local Law Enforcement.

"(7) The Targeted Violence and Terrorism Prevention Director.

"(8) The Officer for Civil Rights and Civil Liberties.

"(9) The Chief Medical Officer.

"(10) The heads of other components or offices of the Department, as determined by the Secretary.".

(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 2023 the following new item:

"Sec. 2024. Memoranda of understanding with departmental components and offices.".

SEC. 608. GRANTS METRICS.

(a) IN GENERAL.—To determine the extent to which grants under sections 2003 and 2004 of the Homeland Security Act of 2002 (6 U.S.C. 603 and 604) have closed capability gaps identified in State Preparedness Reports required under subsection (c) of section 652 of the Post-Katrina Emergency Management Reform Act of 2006 (6 U.S.C. 752; title VI of the Department of Homeland Secu-

rity Appropriations Act, 2007; Public Law 109–295) and Threat and Hazard Identification and Risk Assessments required under subsections (e) and (f) of such sections 2003 and 2004, respectively, as added by this title, from each State and high-risk urban area, the Administrator of the Federal Emergency Management Agency shall conduct and submit to the Committee on Homeland Security and the Committee on Transportation and Infrastructure of the House of Representatives and the Committee on Homeland Security and Governmental Affairs of the Senate an assessment of information provided in such Reports and Assessments.

(b) ASSESSMENT REQUIREMENTS.—The assessment required under subsection (a) shall include a comparison of successive State Preparedness Reports and Threat and Hazard Identification and Risk Assessments that aggregates results across the States and high-risk urban areas.

SEC. 609. GRANT MANAGEMENT BEST PRACTICES.

The Administrator of the Federal Emergency Management Agency shall include in the annual Notice of Funding Opportunity relating to grants under sections 2003 and 2004 of the Homeland Security Act of 2002 (6 U.S.C. 604 and 605) an appendix that includes the following:

(1) A summary of findings identified by the Office of the Inspector General of the Department of Homeland Security in audits of such grants and methods to address areas identified for improvement, including opportunities for technical assistance.

(2) Innovative projects and best practices instituted by grant recipients.

SEC. 610. PROHIBITION ON CONSOLIDATION.

The Secretary of Homeland Security may not implement the National Priorities Security Grant Program or any successor consolidated grant program unless the Secretary receives prior authorization from Congress permitting such implementation.

SEC. 611. MAINTENANCE OF GRANT INVESTMENTS.

Section 2008 of the Homeland Security Act of 2002 (6 U.S.C. 609), as amended by this title, is further amended by adding at the end the following new subsection:

''(h) MAINTENANCE OF EQUIPMENT.—Any applicant for a grant under section 2003 or 2004 seeking to use funds to purchase equipment, including pursuant to paragraphs (3), (4), (5), or (12) of subsection (a) of this section, shall by the time of the receipt of such grant develop a plan for the maintenance of such equipment over its life-

cycle that includes information identifying which entity is responsible for such maintenance.''.

SEC. 612. 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)(A); Public Law 110–53) is amended by inserting ''and associated backfill'' after ''security training''.

SEC. 613. 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 by striking subsection (m) and inserting the following new subsections:

''(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.

''(n) AUTHORIZATION OF APPROPRIATIONS.—There is authorized to be appropriated for grants under this section $200,000,000 for each of fiscal years 2021 through 2022.''.

SEC. 614. COMPTROLLER GENERAL 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 this Act (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 1 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 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. 615. PORT SECURITY GRANT PROGRAM.

Section 70107 of title 46, United States Code, is amended by—

(1) striking subsection (l);

(2) redesignating subsection (m) as subsection (l); and

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

''(n) PERIOD OF PERFORMANCE.—The Secretary shall make funds provided under this section available for use by a recipient of a grant for a period of not less than 36 months.

''(o) AUTHORIZATION OF APPROPRIATIONS.—There is authorized to be appropriated for grants under this section $200,000,000 for each of fiscal years 2021 through 2022.''.

SEC. 616. CYBER PREPAREDNESS.

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

(1) in subsection (c)—

(A) in paragraph (5)(B), by inserting '', including State, local, and regional fusion centers, as appropriate'' before the semicolon at the end;

(B) in paragraph (7), in the matter preceding subparagraph (A), by striking ''information and recommendations'' each place it appears and inserting ''information, recommendations, and best practices''; and

(C) in paragraph (9), by inserting ''best practices,'' after ''defensive measures,''; and

(2) in subsection (d)(1)(B)(ii), by inserting ''and State, local, and regional fusion centers, as appropriate'' before the semicolon at the end.

(b) SENSE OF CONGRESS.—It is the sense of Congress that to facilitate the timely dissemination to appropriate State, local, and private sector stakeholders of homeland security information related to cyber threats, the Secretary of Homeland Security should, to the greatest extent practicable, work to share actionable information in an unclassified form related to such threats.

SEC. 617. OPERATION STONEGARDEN.

(a) IN GENERAL.—Subtitle A of title XX of the Homeland Security Act of 2002 (6 U.S.C. 601 et seq.) is amended by adding at the end the following new section:

''SEC. 2009. OPERATION STONEGARDEN.

''(a) ESTABLISHMENT.—There is established in the Department a program to be known as 'Operation Stonegarden', under which the Secretary, acting through the Administrator, shall make grants to eligible law enforcement agencies, through the State administrative agency, to enhance border security in accordance with this section.

''(a) ELIGIBLE RECIPIENTS.—To be eligible to receive a grant under this section, a law enforcement agency—

1 ''(1) shall be located in—
2 ''(A) a State bordering Canada or Mexico;
3 or
4 ''(B) a State or territory with a maritime
5 border; and
6 ''(2) shall be involved in an active, ongoing,
7 U.S. Customs and Border Protection operation co-
8 ordinated through a U.S. Border Patrol sector of-
9 fice.
10 ''(b) PERMITTED USES.—The recipient of a grant
11 under this section may use such grant for—
12 ''(1) equipment, including maintenance and
13 sustainment costs;
14 ''(2) personnel, including overtime and backfill,
15 in support of enhanced border law enforcement ac-
16 tivities;
17 ''(3) any activity permitted for Operation
18 Stonegarden under the Department of Homeland
19 Security's most recent Homeland Security Grant
20 Program Notice of Funding Opportunity; and
21 ''(4) any other appropriate activity, as deter-
22 mined by the Administrator, in consultation with the
23 Commissioner of U.S. Customs and Border Protec-
24 tion.

"(c) PERIOD OF PERFORMANCE.—The Secretary shall award grants under this section to grant recipients for a period of not less than 36 months.

"(d) REPORT.—For each of fiscal years 2021 and 2022, the Administrator shall submit to the Committee on Homeland Security and Governmental Affairs of the Senate and the Committee on Homeland Security of the House of Representatives a report that contains information on the expenditure of grants made under this section by each grant recipient.

"(e) AUTHORIZATION OF APPROPRIATIONS.—There is authorized to be appropriated $110,000,000 for each of fiscal years 2021 and 2022 for grants under this section.".

(b) CONFORMING AMENDMENT.—Subsection (a) of section 2002 of the Homeland Security Act of 2002 (6 U.S.C. 603) is amended to read as follows:

"(a) GRANTS AUTHORIZED.—The Secretary, through the Administrator, may award grants under sections 2003, 2004, 2009, and 2010 to State, local, and Tribal governments, as appropriate.".

(c) 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 2008 the following new item:

"Sec. 2009. Operation Stonegarden.".

Subtitle B—Communications

SEC. 621. OFFICE OF EMERGENCY COMMUNICATIONS.

The Secretary of Homeland Security may not change the location or reporting structure of the Office of Emergency Communications of the Department of Homeland Security unless the Secretary receives prior authorization from the Committee on Homeland Security of the House of Representatives and the Committee on Homeland Security and Governmental Affairs of the Senate permitting such change.

SEC. 622. RESPONSIBILITIES OF OFFICE OF EMERGENCY COMMUNICATIONS DIRECTOR.

(a) IN GENERAL.—Subsection (c) of section 1801 of the Homeland Security Act of 2002 (6 U.S.C. 571) is amended—

(1) by striking paragraph (3);

(2) by redesignating paragraphs (4) through (16) as paragraphs (3) through (15), respectively;

(3) in paragraph (8), as so redesignated, by striking ", in cooperation with the National Communications System,";

(4) in paragraph (11), as so redesignated, by striking "Assistant Secretary for Grants and Training" and inserting "Administrator of the Federal Emergency Management Agency";

(5) in paragraph (14), as so redesignated, by striking ''and'' at the end;

(6) in paragraph (15), as so redesignated, by striking the period at the end and inserting a semicolon; and

(7) by adding at the end the following new paragraphs:

''(16) administer the Government Emergency Telecommunications Service (GETS) and Wireless Priority Service (WPS) programs, or successor programs; and

''(17) assess the impact of emerging technologies on interoperable emergency communications.''.

(b) PERFORMANCE OF PREVIOUSLY TRANSFERRED FUNCTIONS.—Subsection (d) of section 1801 of the Homeland Security Act of 2002 is amended by—

(1) striking paragraph (2); and

(2) redesignating paragraph (3) as paragraph (2).

SEC. 623. ANNUAL REPORTING ON ACTIVITIES OF THE OFFICE OF EMERGENCY COMMUNICATIONS.

Subsection (f) of section 1801 of the Homeland Security Act of 2002 (6 U.S.C. 571) is amended to read as follows:

1 ''(f) ANNUAL REPORTING OF OFFICE ACTIVITIES.—
2 The Director of the Office of Emergency Communications
3 shall, not later than one year after the date of the enact-
4 ment of this subsection and annually thereafter for each
5 of the next four years, report to the Committee on Home-
6 land Security and the Committee on Energy and Com-
7 merce of the House of Representatives and the Committee
8 on Homeland Security and Governmental Affairs of the
9 Senate on the activities and programs of the Office, in-
10 cluding specific information on efforts to carry out para-
11 graphs (4), (5), and (6) of subsection (c).''.

12 **SEC. 624. NATIONAL EMERGENCY COMMUNICATIONS PLAN.**

13 Section 1802 of the Homeland Security Act of 2002
14 (6 U.S.C. 572) is amended—
15 (1) in subsection (a), in the matter preceding
16 paragraph (1)—
17 (A) by striking '', and in cooperation with
18 the Department of National Communications
19 System (as appropriate),''; and
20 (B) by inserting '', but not less than once
21 every five years,'' after ''periodically''; and
22 (2) in subsection (c)—
23 (A) by redesignating paragraphs (3)
24 through (10) as paragraphs (4) through (11),
25 respectively; and

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

''(3) consider the impact of emerging technologies on the attainment of interoperable emergency communications;''.

SEC. 625. TECHNICAL EDIT.

Paragraph (1) of section 1804(b) of the Homeland Security Act of 2002 (6 U.S.C. 574(b)), in the matter preceding subparagraph (A), by striking ''Assistant Secretary for Grants and Planning'' and inserting ''Administrator of the Federal Emergency Management Agency''.

SEC. 626. PUBLIC SAFETY BROADBAND NETWORK.

The Director of the Cybersecurity and Infrastructure Security Agency of the Department of Homeland Security shall provide to the Committee on Homeland Security and the Committee on Energy and Commerce of the House of Representatives and the Committee on Homeland Security and Governmental Affairs of the Senate information on the Department of Homeland Security's responsibilities related to the development of the nationwide Public Safety Broadband Network authorized in section 6202 of the Middle Class Tax Relief and Job Creation Act of 2012 (47 U.S.C. 1422; Public Law 112–96), including information on efforts by the Department to work with the First Responder Network Authority of the Department of Com-

merce to identify and address cyber risks that could impact the near term or long term availability and operations of such network and recommendations to mitigate such risks.

SEC. 627. COMMUNICATIONS TRAINING.

The Under Secretary for Management of the Department of Homeland Security, in coordination with the appropriate component heads, shall develop a mechanism, consistent with the strategy required pursuant to section 4 of the Department of Homeland Security Interoperable Communications Act (Public Law 114–29; 6 U.S.C. 194 note), to verify that radio users within the Department receive initial and ongoing training on the use of the radio systems of such components, including interagency radio use protocols.

Subtitle C—Federal Emergency Management Agency (FEMA)

SEC. 631. SHORT TITLE.

This subtitle may be cited as the ''FEMA Reauthorization Act of 2019''.

SEC. 632. REAUTHORIZATION OF FEDERAL EMERGENCY MANAGEMENT AGENCY.

Section 699 of the Post-Katrina Emergency Management Reform Act of 2006 (Public Law 109–295; 6 U.S.C. 811) is amended—

(1) by striking ''administration and operations'' each place it appears and inserting ''management and administration'';

(2) in paragraph (2), by striking ''; and'';

(3) in paragraph (3), by striking the period and inserting ''; and''; and

(4) by adding at the end the following:

''(4) for fiscal year 2021, $1,124,242,980; and

''(6) for fiscal year 2022, $1,146,727,840.''.

SEC. 633. NATIONAL DOMESTIC PREPAREDNESS CONSORTIUM.

Section 1204 of the Implementing Recommendations of the 9/11 Commission Act (6 U.S.C. 1102) is amended—

(1) in subsection (b)(4), by striking ''Rescue'' and inserting ''Recovery'';

(2) in subsection (c), by inserting ''to the extent practicable, provide training in settings that simulate real response environments, such as urban areas,'' after ''levels,'';

(3) in subsection (d), by striking paragraphs (1) and (2) and inserting the following:

''(1) for the Center for Domestic Preparedness—

''(A) $68,131,920 for fiscal year 2021; and

"(B) $69,494,558 for fiscal year 2022; and

"(2) for the members referred to in paragraphs (2) through (7) of subsection (b)—

"(A) $103,020,000 for fiscal year 2021; and

"(B) $105,080,400 for fiscal year 2022."; and

(4) in subsection (e) by striking—

(A) "each of the following entities" and inserting "members enumerated in section (b)";

(B) "2007—" and inserting "2015."; and

(C) paragraphs (1) through (5).

SEC. 634. RURAL DOMESTIC PREPAREDNESS CONSORTIUM.

(a) IN GENERAL.—The Secretary of Homeland Security is authorized to establish a Rural Domestic Preparedness Consortium within the Department of Homeland Security consisting of universities and nonprofit organizations qualified to provide training to emergency response providers from rural communities.

(b) DUTIES.—The Rural Domestic Preparedness Consortium authorized under subsection (a) shall identify, develop, test, and deliver training to State, local, and Tribal emergency response providers from rural communities, provide on-site and mobile training, and facilitate the de-

1 livery of training by the training partners of the Depart-
2 ment of Homeland Security.
3 (c) AUTHORIZATION OF APPROPRIATIONS.—Of
4 amounts appropriated for Continuing Training Grants of
5 the Department of Homeland Security, $5,000,000 is au-
6 thorized to be used for the Rural Domestic Preparedness
7 Consortium authorized under subsection (a).

8 **SEC. 635. CENTER FOR FAITH-BASED AND NEIGHBORHOOD**
9 **PARTNERSHIPS.**

10 (a) IN GENERAL.—Title V of the Homeland Security
11 Act of 2002 (6 U.S.C. 311 et seq.) is amended by adding
12 at the end the following new section:

13 **"SEC. 529. CENTER FOR FAITH-BASED AND NEIGHBORHOOD**
14 **PARTNERSHIPS.**

15 "(a) IN GENERAL.—There is established in the Agen-
16 cy a Center for Faith-Based and Neighborhood Partner-
17 ships, headed by a Director appointed by the Secretary.
18 "(b) MISSION.—The mission of the Center shall be
19 to develop and coordinate Departmental outreach efforts
20 with faith-based and community organizations and serve
21 as a liaison between such organizations and components
22 of the Department for activities related to securing facili-
23 ties, emergency preparedness and response, and com-
24 bating human trafficking.

1 ''(c) RESPONSIBILITIES.—In support of the mission
2 of the Center for Faith-Based and Neighborhood Partner-
3 ships, the Director shall—
4 ''(1) develop exercises that engage faith-based
5 and community organizations to test capabilities for
6 all hazards, including active shooter incidents;
7 ''(2) coordinate the delivery of guidance and
8 training to faith-based and community organizations
9 related to securing their facilities against natural
10 disasters, acts of terrorism, and other man-made
11 disasters;
12 ''(3) conduct outreach to faith-based and com-
13 munity organizations regarding guidance, applicable
14 grant programs, training, and exercises and Depart-
15 mental capabilities available to assist faith-based
16 and community organizations to secure their facili-
17 ties against natural disasters, acts of terrorism, and
18 other man-made disasters;
19 ''(4) facilitate engagement and coordination
20 among the emergency management community and
21 faith-based and community organizations;
22 ''(5) deliver training and technical assistance to
23 faith-based and community-based organizations and
24 provide subject-matter expertise related to anti-
25 human trafficking efforts to help communities suc-

cessfully partner with other Blue Campaign components; and

"(6) perform any other duties as assigned by the Administrator.".

(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 528 the following new item:

"Sec. 529. Center for Faith-Based and Neighborhood Partnerships.".

SEC. 636. EMERGENCY SUPPORT FUNCTIONS.

(a) UPDATE.—Paragraph (13) of section 504(a) of the Homeland Security Act of 2002 (6 U.S.C. 314(a)) is amended by inserting ", periodically updating (but not less often than once every five years)," after "administering".

(b) EMERGENCY SUPPORT FUNCTIONS.—Section 653 of the Post-Katrina Emergency Management Reform Act of 2006 (6 U.S.C. 753; title VI of the Department of Homeland Security Appropriations Act, 2007; Public Law 109–295) is amended—

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

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

"(d) COORDINATION.—The President, acting through the Administrator, shall develop and provide to Federal departments and agencies with coordinating, primary, or

supporting responsibilities under the National Response Framework performance metrics to ensure readiness to execute responsibilities under the emergency support functions of such Framework.''.

SEC. 637. REVIEW OF NATIONAL INCIDENT MANAGEMENT SYSTEM.

Paragraph (2) of section 509(b) of the Homeland Security Act of 2002 (6 U.S.C. 319(b)) is amended, in the matter preceding subparagraph (A), by inserting '', but not less often than once every five years,'' after ''periodically''.

SEC. 638. REMEDIAL ACTION MANAGEMENT PROGRAM.

Section 650 of the Post-Katrina Emergency Management Reform Act of 2006 (6 U.S.C. 750; title VI of the Department of Homeland Security Appropriations Act, 2007; Public Law 109–295) is amended to read as follows:

''SEC. 650. REMEDIAL ACTION MANAGEMENT PROGRAM.

''(a) IN GENERAL.—The Administrator, in coordination with the National Council on Disability and the National Advisory Council, shall establish a remedial action management program to—

''(1) analyze training, exercises, and real world events to identify lessons learned, corrective actions, and best practices;

1 ''(2) generate and disseminate, as appropriate,
2 the lessons learned, corrective actions, and best
3 practices referred to in paragraph (1); and
4 ''(3) conduct remedial action tracking and long-
5 term trend analysis.
6 ''(b) FEDERAL CORRECTIVE ACTIONS.—The Admin-
7 istrator, in coordination with the heads of appropriate
8 Federal departments and agencies, shall utilize the pro-
9 gram established pursuant to subsection (a) to collect in-
10 formation on corrective actions identified by such Federal
11 departments and agencies during exercises and the re-
12 sponse to natural disasters, acts of terrorism, and other
13 man-made disasters, and shall, not later than one year
14 after the date of the enactment of this section and annu-
15 ally thereafter for each of the next four years, submit to
16 Congress a report on the status of such corrective actions.
17 ''(c) DISSEMINATION OF AFTER ACTION REPORTS.—
18 The Administrator shall provide electronically, to the max-
19 imum extent practicable, to Congress and Federal, State,
20 local, Tribal, and private sector officials after-action re-
21 ports and information on lessons learned and best prac-
22 tices from responses to acts of terrorism, natural disas-
23 ters, capstone exercises conducted under the national exer-
24 cise program under section 648(b), and other emergencies
25 or exercises.''.

SEC. 639. STRATEGIC HUMAN CAPITAL PLAN.

Subsection (c) of section 10102 of title 5, United States Code, is amended by striking ''2007'' and inserting ''2021''.

SEC. 640. OFFICE OF DISABILITY INTEGRATION AND COORDINATION.

(a) OFFICE OF DISABILITY INTEGRATION AND COORDINATION.—

(1) IN GENERAL.—Section 513 of the Homeland Security Act of 2002 (6 U.S.C. 321b) is amended to read as follows:

''SEC. 513. OFFICE OF DISABILITY INTEGRATION AND COORDINATION.

''(a) IN GENERAL.—There is established within the Federal Emergency Management Agency an Office of Disability Integration and Coordination, which shall be headed by a Director.

''(b) MISSION.—The mission of the Office is to ensure that individuals with disabilities and other access and functional needs are included in emergency management activities throughout the Agency by providing guidance, tools, methods, and strategies for the purpose of equal physical program and effective communication access.

''(c) RESPONSIBILITIES.—In support of the mission of the Office, the Director shall—

1 ''(1) provide guidance and coordination on mat-
2 ters related to individuals with disabilities in emer-
3 gency planning requirements and relief efforts in the
4 event of a natural disaster, act of terrorism, or other
5 man-made disaster;
6 ''(2) oversee Office staff and personnel respon-
7 sible for disability integration in each regional office
8 with respect to carrying out the mission of the Of-
9 fice;
10 ''(3) liaise with the staff of the Agency includ-
11 ing nonpermanent employees, organizations rep-
12 resenting individuals with disabilities, other agencies
13 of the Federal Government, and State, local, and
14 Tribal government authorities regarding the needs of
15 individuals with disabilities in emergency planning
16 requirements and relief efforts in the event of a nat-
17 ural disaster, act of terrorism, or other man-made
18 disaster;
19 ''(4) consult with organizations representing in-
20 dividuals with disabilities about access and func-
21 tional needs in emergency planning requirements
22 and relief efforts in the event of a natural disaster,
23 act of terrorism, or other man-made disaster;

1 ''(5) ensure the coordination and dissemination
2 of best practices and model evacuation plans for in-
3 dividuals with disabilities;
4 ''(6) collaborate with Agency leadership respon-
5 sible for training to ensure that qualified experts de-
6 velop easily accessible training materials and a cur-
7 riculum for the training of emergency response pro-
8 viders, State, local, and Tribal government officials,
9 and others on the needs of individuals with disabil-
10 ities;
11 ''(7) coordinate with the Emergency Manage-
12 ment Institute, Center for Domestic Preparedness,
13 Center for Homeland Defense and Security, U.S.
14 Fire Administration, National Exercise Program,
15 and National Domestic Preparedness Consortium to
16 ensure that content related to persons with disabil-
17 ities, access and functional needs, and children are
18 integrated into existing and future emergency man-
19 agement trainings;
20 ''(8) promote the accessibility of telephone hot-
21 lines and websites regarding emergency prepared-
22 ness, evacuations, and disaster relief;
23 ''(9) work to ensure that video programming
24 distributors, including broadcasters, cable operators,
25 and satellite television services, make emergency in-

formation accessible to individuals with hearing and vision disabilities;

''(10) ensure the availability of accessible transportation options for individuals with disabilities in the event of an evacuation;

''(11) provide guidance and implement policies to ensure that the rights and feedback of individuals with disabilities regarding post-evacuation residency and relocation are respected;

''(12) ensure that meeting the needs of individuals with disabilities are included in the components of the national preparedness system established under section 644 of the Post-Katrina Emergency Management Reform Act of 2006 (Public Law 109–295; 120 Stat. 1425; 6 U.S.C. 744); and

''(13) perform any other duties as assigned by the Administrator.

''(d) DIRECTOR.—After consultation with organizations representing individuals with disabilities, the Administrator shall appoint a Director. The Director shall report directly to the Administrator, in order to ensure that the needs of individuals with disabilities are being properly addressed in emergency preparedness and disaster relief.

''(e) ORGANIZATIONS REPRESENTING INDIVIDUALS WITH DISABILITIES DEFINED.—For purposes of this sec-

1 tion, the term 'organizations representing individuals with
2 disabilities' shall mean the National Council on Disabil-
3 ities and the Interagency Coordinating Council on Pre-
4 paredness and Individuals with Disabilities, among other
5 appropriate disability organizations.''.

6 (2) CLERICAL AMENDMENT.—The table of con-
7 tents in section 1(b) of such Act is amended by
8 striking the item relating to section 513 and insert-
9 ing the following new item:

''Sec. 513. Office of Disability Integration and Coordination.''.

10 (b) REPORTING.—

11 (1) REPORT TO CONGRESS.—Not later than
12 120 days after the date of the enactment of this sec-
13 tion, the Administrator shall submit to Congress a
14 report on the funding and staffing needs of the Of-
15 fice of Disability Integration and Coordination under
16 section 513 of the Homeland Security Act of 2002,
17 as amended by subsection (a).

18 (2) COMPTROLLER GENERAL REVIEW.—Not
19 later than 120 days after the date of the submission
20 of the report under paragraph (1), the Comptroller
21 General of the United States shall review the report
22 to evaluate whether the funding and staffing needs
23 described in the report are sufficient to support the
24 activities of the Office of Disability Integration and
25 Coordination.

SEC. 641. FEMA SENIOR LAW ENFORCEMENT ADVISOR.

(a) IN GENERAL.—Title V of the Homeland Security Act of 2002 (6 U.S.C. 311 et seq.), as amended by this title, is further amended by adding at the end the following new section:

"SEC. 530. SENIOR LAW ENFORCEMENT ADVISOR.

"(a) ESTABLISHMENT.—There is established in the Agency a Senior Law Enforcement Advisor to serve as a qualified expert to the Administrator for the purpose of strengthening the Agency's coordination among State, local, and Tribal law enforcement.

"(b) QUALIFICATIONS.—The Senior Law Enforcement Advisor shall have an appropriate background with experience in law enforcement, intelligence, information sharing, and other emergency response functions.

"(c) RESPONSIBILITIES.—The Senior Law Enforcement Advisor shall—

"(1) coordinate on behalf of the Administrator with the Office for State and Local Law Enforcement under section 2006 for the purpose of ensuring State, local, and Tribal law enforcement receive consistent and appropriate consideration in policies, guidance, training, and exercises related to preventing, preparing for, protecting against, and responding to natural disasters, acts of terrorism, and other man-made disasters within the United States;

"(2) work with the Administrator and the Office for State and Local Law Enforcement under section 2006 to ensure grants to State, local, and Tribal government agencies, including programs under sections 2003, 2004, and 2006(a), appropriately focus on terrorism prevention activities; and

"(3) serve other appropriate functions as determined by the Administrator.".

(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 529, as added by this title, the following new item:

"Sec. 530. Senior Law Enforcement Advisor.".

SEC. 642. TECHNICAL AMENDMENTS TO NATIONAL EMERGENCY MANAGEMENT.

(a) HOMELAND SECURITY ACT OF 2002.—Title V of the Homeland Security Act of 2002 (6 U.S.C. 501 et seq.) is amended—

(1) in section 501(8) (6 U.S.C. 311(8))—

(A) by striking "National Response Plan" each place it appears and inserting "National Response Framework"; and

(B) by striking "502(a)(6)" and inserting "504(a)(6)";

(2) in section 503(b)(2)(A) (6 U.S.C. 313) by inserting ''and incidents impacting critical infrastructure'' before the semicolon;

(3) in section 504(a) (6 U.S.C. 314(a))—

(A) in paragraph (3) by striking '', including—'' and inserting ''(that includes incidents impacting critical infrastructure), including—'';

(B) in paragraph (4) by inserting '', including incidents impacting critical infrastructure'' before the semicolon;

(C) in paragraph (5) by striking ''and local'' and inserting ''local, and Tribal'';

(D) in paragraph (6) by striking ''national response plan'' and inserting ''national response framework, which shall be reviewed and updated as required but not less than every 5 years'';

(E) by redesignating paragraphs (7) through (21) as paragraphs (8) through (22), respectively;

(F) by inserting after paragraph (6) the following:

''(7) developing integrated frameworks, to include consolidating existing Government plans addressing prevention, protection, mitigation, and re-

1 covery with such frameworks reviewed and updated
2 as required, but not less than every 5 years;''; and
3 (G) in paragraph (14), as so redesignated,
4 by striking ''National Response Plan'' each
5 place it appears and inserting ''National Re-
6 sponse Framework'';
7 (4) in section 507 (6 U.S.C. 317)—
8 (A) in subsection (c)—
9 (i) in paragraph (2)(E), by striking
10 ''National Response Plan'' and inserting
11 ''National Response Framework''; and
12 (ii) in paragraph (3)(A), by striking
13 ''National Response Plan'' and inserting
14 ''National Response Framework''; and
15 (B) in subsection (f)(1)(G), by striking
16 ''National Response Plan'' and inserting ''Na-
17 tional Response Framework'';
18 (5) in section 508 (6 U.S.C. 318)—
19 (A) in subsection (b)(1), by striking ''Na-
20 tional Response Plan'' and inserting ''National
21 Response Framework''; and
22 (B) in subsection (d)(2)(A), by striking
23 ''The Deputy Administrator, Protection and
24 National Preparedness'' and inserting ''A Dep-
25 uty Administrator'';

(6) in section 509 (6 U.S.C. 319)—

(A) in subsection (b)—

(i) in paragraph (1)—

(I) by striking ''National Response Plan'' and inserting ''National Response Framework, National Protection Framework, National Prevention Framework, National Mitigation Framework, National Recovery Framework'';

(II) by striking ''successor'' and inserting ''successors''; and

(III) by striking ''plan'' at the end of that paragraph and inserting ''framework''; and

(ii) in paragraph (2), by striking ''National Response Plan'' each place it appears and inserting ''National Response Framework''; and

(B) in subsection (c)(1)—

(i) in subparagraph (A)—

(I) by striking ''NATIONAL RESPONSE PLAN'' in the header and inserting ''NATIONAL RESPONSE FRAMEWORK''; and

(II) by striking ''National Response Plan'' in the text and inserting ''National Response Framework''; and

(ii) in subparagraph (B), by striking ''National Response Plan'' and inserting ''National Response Framework'';

(7) in section 510 (6 U.S.C. 320)—

(A) in subsection (a), by striking ''enter into a memorandum of understanding'' and inserting ''partner'';

(B) in subsection (b)(1)(A), by striking ''National Response Plan'' and inserting ''National Response Framework''; and

(C) in subsection (c), by striking ''National Response Plan'' and inserting ''National Response Framework'';

(8) in section 515(c)(1) (6 U.S.C. 321d(c)(1)), by striking ''and local'' each place it appears and inserting '', local, and Tribal'';

(9) by striking section 524 (6 U.S.C. 321m); and

(10) in section 525(a) (6 U.S.C. 321n), by striking ''Secretary'' and inserting ''Administrator''.

(b) POST-KATRINA EMERGENCY MANAGEMENT REFORM ACT OF 2006.—

(1) CITATION CORRECTION.—Section 602(13) of the Post-Katrina Emergency Management Reform Act of 2006 (6 U.S.C. 701(13)) is amended by striking ''502(a)(6)'' and inserting ''504(a)(6)''.

(2) CHANGE OF REFERENCE.—Chapter 1 of subtitle C of title VI of the Post-Katrina Emergency Management Reform Act of 2006 (Public Law 109–295) is amended by striking ''National Response Plan'' each place it appears and inserting ''National Response Framework''.

(c) SAVINGS CLAUSE.—The amendments made by subsection (a) to section 503(b)(2)(A) and paragraphs (3) and (4) of section 504(a) of the Homeland Security Act of 2002 may not be construed as affecting the authority, existing on the day before the date of enactment of this division, of any other component of the Department of Homeland Security or any other Federal department or agency.

Subtitle D—Genome Editing Threat Assessment

SEC. 651. GENOME EDITING THREAT ASSESSMENT.

(a) IN GENERAL.—Not later than 180 days after the date of the enactment of this Act, the Assistant Secretary for the Countering Weapons of Mass Destruction Office of the Department of Homeland Security, in coordination

with the Under Secretary for Intelligence and Analysis of the Department, the Under Secretary for the Science and Technology Directorate of the Department, and other Federal partners, as appropriate, shall develop a threat assessment on the potential homeland security vulnerabilities associated with genome modification and editing. Such threat assessment shall include information relating to the following:

(1) The dual-use of emerging biotechnology.

(2) The ability of gene editing to maliciously proliferate infectious diseases and pandemics on human, animal, and plant populations.

(3) The cybersecurity vulnerabilities in computer systems analyzing genomic data.

(4) Privacy concerns associated with analyzing genomic data.

(b) RECOMMENDATIONS.—Upon completion of the threat assessment required under subsection (a), the Secretary of Homeland Security shall make a determination if any changes to future operations of the Department of Homeland Security are required to address security vulnerabilities identified in such assessment.

(c) REPORT.—Not later than 60 days after the completion of the threat assessment required under subsection (a), the Secretary of Homeland Security shall, consistent

with the protection of classified information, report to the Committee on Homeland Security of the House of Representatives and the Committee on Homeland Security and Governmental Affairs of the Senate on the findings of such threat assessment, any identified recommendations, plans for incorporating such recommendations into future operations of the Department of Homeland Security, and any proposed legislative changes informed by such threat assessment.

TITLE VII—PANDEMIC PREPAREDNESS

SEC. 701. CHIEF MEDICAL OFFICER.

Section 1931 of the Homeland Security Act of 2002 (6 U.S.C. 587) is amended—

(1) in subsection (c)—

(A) in the matter preceding paragraph (1), by inserting ''and shall establish medical and human, animal, and occupational health exposure policy, guidance, strategies, and initiatives,'' before ''including—'';

(B) in paragraph (1), by inserting before the semicolon at the end the following: '', including advice on how to prepare for, protect against, respond to, recover from, and mitigate against the medical effects of terrorist attacks

or other high consequence events utilizing chemical, biological, radiological, or nuclear agents or explosives'';

(C) in paragraph (2), by inserting before the semicolon at the end the following: '', including coordinating the Department's policy, strategy, and preparedness for pandemics and emerging infectious diseases'';

(D) in paragraph (4)—

(i) by inserting ''emergency medical services and medical first responder stakeholders,'' after ''the medical community,''; and

(ii) by striking ''and'' at the end;

(E) by redesignating paragraph (5) as paragraph (9); and

(F) by inserting after paragraph (4) the following new paragraphs:

''(5) ensuring that the workforce of the Department has evidence-based policy, standards, requirements, and metrics for operational medicine programs;

''(6) directing and maintaining a coordinated system for medical support for the Department's operational activities;

1 ''(7) providing oversight of the Department's
2 medical programs and providers, including—
3 ''(A) reviewing and maintaining
4 verification of the accreditation of the Depart-
5 ment's health provider workforce;
6 ''(B) developing quality assurance and clin-
7 ical policy, requirements, standards, and
8 metrics for all medical and health activities of
9 the Department;
10 ''(C) providing oversight of medical records
11 systems for employees and individuals in the
12 Department's care and custody; and
13 ''(D) providing medical direction for emer-
14 gency medical services activities of the Depart-
15 ment;
16 ''(8) as established under section 1932, main-
17 taining a medical countermeasures stockpile and dis-
18 pensing system, as necessary, to facilitate personnel
19 readiness, and protection for the Department's em-
20 ployees and working animals and individuals in the
21 Department's care and custody in the event of a
22 chemical, biological, radiological, nuclear, or explo-
23 sives attack, naturally occurring disease outbreak, or
24 pandemic; and''; and

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

''(d) MEDICAL LIAISONS.—The Chief Medical Officer may provide medical liaisons to the components of the Department to provide subject matter expertise on medical and public health issues and a direct link to the Chief Medical Officer. Such expertise may include the following:

''(1) Providing guidance on health and medical aspects of policy, planning, and operations.

''(2) Supporting the development and alignment of medical and health systems.

''(3) Identifying—

''(A) common gaps in medical and health standards, policy, or guidance; and

''(B) enterprise solutions to bridge such gaps.''.

SEC. 702. 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 and individuals in the Department's

care and custody, 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 Department-wide 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 on 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;

1 ''(6) provide training to Department employees
2 on medical countermeasure dispensing; and
3 ''(7) support dispensing exercises.
4 ''(c) MEDICAL COUNTERMEASURES WORKING
5 GROUP.—The Chief Medical Officer shall establish a med-
6 ical countermeasures working group comprised of rep-
7 resentatives from appropriate components and offices of
8 the Department to ensure that medical countermeasures
9 standards are maintained and guidance is consistent.
10 ''(d) MEDICAL COUNTERMEASURES MANAGE-
11 MENT.—Not later than 180 days after the date of the en-
12 actment of this section, the Chief Medical Officer shall de-
13 velop and submit to the Secretary an integrated logistics
14 support plan for medical countermeasures, including—
15 ''(1) a methodology for determining the ideal
16 types and quantities of medical countermeasures to
17 stockpile and how frequently such methodology shall
18 be reevaluated;
19 ''(2) a replenishment plan; and
20 ''(3) inventory tracking, reporting, and rec-
21 onciliation procedures for existing stockpiles and
22 new medical countermeasure purchases.
23 ''(e) STOCKPILE ELEMENTS.—In determining the
24 types and quantities of medical countermeasures to stock-

pile 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 Chief Medical Officer 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 on progress in achieving the requirements of this section.".

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

"Sec. 1932. Medical countermeasures.".

SEC. 703. PERSONAL PROTECTIVE EQUIPMENT.

(a) DEFINITIONS.—In this section:

(1) APPROPRIATE CONGRESSIONAL COMMITTEES.—The term "appropriate congressional committees" means the Committee on Homeland Security of the House of Representatives and the Committee on Homeland Security and Governmental Affairs of the Senate.

(2) DEPARTMENT.—The term ''Department'' means the Department of Homeland Security.

(3) PERSONAL PROTECTIVE EQUIPMENT.—The term ''personal protective equipment'' includes protective gloves, masks, and any additional protective equipment determined appropriate by the Secretary.

(4) SECRETARY.—The term ''Secretary'' means the Secretary of Homeland Security.

(b) AVAILABILITY OF PERSONAL PROTECTIVE EQUIPMENT FOR CERTAIN DEPARTMENT PERSONNEL.—

(1) IN GENERAL.—Not later than 90 days after the date of the enactment of this Act, the Secretary shall ensure the availability of an adequate supply of personal protective equipment to equip personnel of the Department and each component conducting operations requiring contact with the public for use during the COVID–19 global pandemic. Such personnel include the following:

(A) Transportation Security Officers.

(B) Explosives Detection Canine Handlers.

(C) Federal Air Marshals.

(D) Transportation Security Inspectors.

(E) Administration personnel involved in operations of Visual Intermodal Prevention and Response teams.

(F) U.S. Border Patrol agents.

(G) U.S. Customs and Border Protection officers.

(H) Air and Marine Officers.

(I) U.S. Border Patrol Processing Coordinators.

(J) Officers of the Federal Protective Service.

(K) Secret Service Agents and officers.

(L) U.S. Immigration and Customs Enforcement officers.

(M) Any other personnel determined appropriate by the Secretary.

(2) JOB HAZARD ANALYSIS.—Not later than 30 days after the date of the enactment of this Act, each Department component head shall—

(A) ensure the job hazard analysis of each such component identifies the regular duties and tasks required of relevant personnel to determine the amount of personal protective equipment required per shift to conduct specified duties and tasks; and

(B) provide to the Secretary such analysis.

(3) STORAGE.—Not later than 30 days after the date of the enactment of this Act, each Depart-

ment component head shall identify and implement appropriate best practices for storing personal protective equipment.

(4) MEASURES TO PROTECT CERTAIN FRONTLINE PERSONNEL.—Not later than 60 days after the date of the enactment of this Act, each Department component head shall identify and implement measures to augment existing Department facilities and vehicles to protect frontline Department personnel regularly interacting with or transporting individuals in the public. Such measures shall include the implementation of technologies such as plexiglass barriers, biometric technology, computed tomography, detection-at-range, and credential authentication technology utilizing digital camera technology.

(5) POLICIES.—Not later than 60 days after the date of the enactment of this Act, the Secretary shall develop or update, as appropriate, policies for the workforce of the Department related to the use and potential reuse and availability of personal protective equipment.

(6) REPORT TO CONGRESS.—The Secretary shall report to the appropriate congressional committees regarding the implementation of this subsection.

(c) COVID-19 AFTER-ACTION REVIEW.—Not later than 180 days after the date of the enactment of this Act, the Secretary shall submit to the appropriate congressional committees an after-action review to examine the Department's response and mitigation efforts related to the COVID–19 global pandemic. Such review shall include information relating to the following:

(1) The overall preparedness of the Department and each of the Department components to respond to the COVID–19 global pandemic, including preparedness to continue to fulfill its mission and protect Department personnel, the public, the transportation system, ports of entry, and the border.

(2) Communication challenges related to effectively engaging with the public, Department personnel, and appropriate Federal, State, local, Tribal, and industry stakeholders.

(3) The effectiveness of existing authorities allowing the Department to utilize weather and safety leave policies, hazard pay, or other personnel management policies to protect Department personnel.

(4) Impacts on security functions, operations, and other homeland security missions.

(5) The availability of personal protective equipment for Department personnel and individuals in the custody of the Department.

(6) The extent to which technologies to promote less contact between Department personnel and the public, such as the technologies referred to in subsection (d), were implemented, and any challenges or impediments to such implementation.

(7) Recommendations for action to improve the preparedness of the Department for future crises and pandemics.

SEC. 704. TELEWORKING ASSESSMENT.

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 the capabilities of the Department of Homeland Security to support Department-wide teleworking activity during the COVID-19 pandemic. Such review shall include the following:

(1) A description of how many employees in each component of the Department engaged in teleworking prior to the COVID-19 pandemic and how many engaged in teleworking beginning in March 2020.

(2) An evaluation of the capabilities of each of the components to support remote teleworking activities during the COVID-19 pandemic.

(3) An evaluation of the security protocols and guidance developed by the Department and the level of compliance by employees with such protocols.

(4) An assessment of the major issues encountered by each component during the transition to teleworking due to the COVID-19 pandemic.

(5) An assessment of the availability of assistance with teleworking capabilities during the COVID-19 pandemic.

(6) An assessment of the capability of the Department to support teleworking by employees engaged in responsibilities that require the review of classified materials.

(7) Recommendations for improving teleworking capabilities for all employees, including for employees engaged in responsibilities that require the review of classified materials.

SEC. 705. TRANSPORTATION SECURITY PUBLIC HEALTH THREAT PREPAREDNESS.

(a) DEFINITIONS.—In this section:

(1) ADMINISTRATION; TSA.—The terms ''Administration'' and ''TSA'' mean the Transportation Security Administration.

(2) ADMINISTRATOR.—The term ''Administrator'' means the Administrator of the Transportation Security Administration.

(3) APPROPRIATE CONGRESSIONAL COMMITTEES.—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.

(4) DEPARTMENT.—The terms ''Department'' means the Department of Homeland Security.

(b) AUTHORIZATION OF TSA PERSONNEL DETAILS.—

(1) IN GENERAL.—Pursuant to section 114(m) of title 49, United States Code, the Administrator is authorized to provide Administration personnel to other components of the Department and other Federal agencies to improve coordination with such components and such agencies to prepare for, protect

against, and respond to public health threats to transportation security.

(2) STRATEGY.—Not later than 180 days after the date of the enactment of this Act, the Administrator shall brief the appropriate congressional committees regarding a strategy to improve coordination with other components of the Department and other Federal agencies to prepare for, protect against, and respond to public health threats to transportation security.

(c) TSA PREPAREDNESS.—

(1) RISK ANALYSIS.—To the extent possible and in consultation with transportation security stakeholders, the Administrator shall conduct an analysis of transportation sector preparedness for public health threats. Such analysis shall assess at a minimum the following:

(A) The risks of public health threats to transportation security, including to transportation hubs, transportation security stakeholders, Administration personnel, and passengers.

(B) Information sharing challenges among relevant components of the Department, other

Federal agencies, international partners, and transportation security stakeholders.

(C) Impacts on changes to Administration policies and procedures for screening passengers and property.

(2) BRIEFING TO CONGRESS.—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:

(A) The risk analysis required under paragraph (1).

(B) Technologies necessary to advance toward a contactless checkpoint to better protect from future public health threats Administration personnel, passengers, airport personnel, and authorized personnel who pass through airport screening areas.

(C) Policies and procedures implemented by the Administration and transportation security stakeholders to protect from public health threats Administration personnel, passengers, airport personnel, and authorized personnel who pass through airport screening areas, as well as future plans for additional measures relating to such protection.

(D) The status of existing or future planned security directives or emergency amendments to air carrier security requirements for flights from international points.

(E) How the Administration coordinates and shares information with relevant domestic and international partners during a public health threat, and how such coordination may be improved.

SEC. 706. SECURING CRITICAL SUPPLIES.

(a) STRATEGY TO PREVENT A SHORTAGE OF ITEMS DETERMINED TO BE CRITICAL TO SURVIVAL DURING A CRISIS AND SAFEGUARD THE SUPPLY CHAINS OF SUCH ITEMS.—Not later than 180 days after the date of the enactment of this Act, the Secretary, acting through the Under Secretary and the Director, shall—

(1) identify items determined by the Secretary to be critical to survival during a crisis resulting from a terrorist attack, pandemic, or natural disaster;

(2) assess the activities of the Department with respect to the prevention of a shortage of items;

(3) assess vulnerabilities in the supply chain for such items, which vulnerabilities may be exploited by individuals, entities, or foreign terrorist organiza-

tions that may have an adversarial relationship with the United States; and

(4) develop and submit to the appropriate congressional committees a—

(A) report containing a strategy to prevent such a shortage based upon the assessments required under paragraph (2); and

(B) classified annex to the report required under subparagraph (A) relating to a strategy to prevent the exploitation of vulnerabilities in the supply chain for such items based upon the assessment required under paragraph (3).

(b) MATTERS INCLUDED.—The strategies required under subsection (a) shall include—

(1) an identification of items that the Secretary determines to be critical to survival, including—

(A) food and water;

(B) prescription medication;

(C) medical supplies; and

(D) energy infrastructure and supplies;

(2) an examination of whether the source of any such item is foreign-owned, controlled, or influenced by a country that may have an adversarial relationship with the United States; and

(3) recommendations with respect to steps the Department could take to—

(A) ensure the availability of such items; and

(B) safeguard from exploitation by individuals, entities, or foreign terrorist organizations the supply chain for such items.

(c) DEFINITIONS.—In this section:

(1) APPROPRIATE CONGRESSIONAL COMMITTEES.—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 of the Senate.

(2) DEPARTMENT.—The term ''Department'' means the Department of Homeland Security.

(3) DIRECTOR.—The term ''Director'' means the Director of the Cybersecurity and Infrastructure Security Agency of the Department of Homeland Security.

(4) SECRETARY.—The term ''Secretary'' means the Secretary of Homeland Security.

(5) UNDER SECRETARY.—The term ''Under Secretary'' means the Under Secretary of Intel-

1 ligence and Analysis of the Department of Home-
2 land Security.