

.....
(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.

1 *Be it enacted by the Senate and House of Representa-*
2 *tives of the United States of America in Congress assembled,*

3 **SECTION 1. SHORT TITLE; TABLE OF CONTENTS.**

4 (a) SHORT TITLE.—This Act may be cited as the
5 “Keep America Secure Act”.

6 (b) TABLE OF CONTENTS.—The table of contents for
7 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 territorial 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.

1 SEC. 2. AUTHORIZATION OF APPROPRIATIONS.

2 There is authorized to be appropriated for the nec-
3 essary expenses of the Department of Homeland Security
4 authorized by this Act, the amendments made by this Act,
5 and other provisions of law (including relevant provisions
6 of title 49, United States Code, and the Homeland Secu-
7 rity Act of 2002 (6 U.S.C. 101 et seq.))—

8 (1) \$59,100,000,000 for fiscal year 2021, of
9 which—

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

1 (B) \$7,917,936,000 shall be for the Trans-
2 portation Security Administration as provided
3 by section 114(w) of title 49, United States
4 Code; and

5 (2) \$60,200,000,000 for fiscal year 2022, of
6 which \$20,477,721,840 shall be for grants and agen-
7 cy expenditures as provided in titles III, IV, V, and
8 VI and the amendments made by such titles.

9 **TITLE I—MANAGEMENT REFORM**
10 **AND ACCOUNTABILITY**
11 **Subtitle A—Headquarters**
12 **Operation**

13 **SEC. 101. HOMELAND SECURITY ENTERPRISE DEFINED.**

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

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

19 (2) by inserting after paragraph (8) the fol-
20 lowing new paragraph (9):

21 “(9) The term ‘homeland security enterprise’
22 means any relevant governmental or nongovern-
23 mental entity involved in homeland security, includ-
24 ing a Federal, State, or local government official,

1 private sector representative, academic, or other pol-
2 icy expert.”.

3 **SEC. 102. FUNCTIONS AND COMPONENTS OF HEAD-**
4 **QUARTERS OF DEPARTMENT OF HOMELAND**
5 **SECURITY.**

6 Section 102 of the Homeland Security Act of 2002
7 (6 U.S.C. 112) is amended—

8 (1) in subsection (b)—

9 (A) in paragraph (2), by striking “and”
10 after the semicolon at the end;

11 (B) in paragraph (3), by striking the pe-
12 riod and inserting “; and”; and

13 (C) by adding at the end the following:

14 “(4) may enter into agreements with govern-
15 ments of other countries, in consultation with the
16 Secretary of State and international nongovern-
17 mental organizations, in order to achieve the mis-
18 sions of the Department.”; and

19 (2) in subsection (c), in the matter preceding
20 paragraph (1), by striking “through the Office of
21 State and Local Coordination (established under sec-
22 tion 801)” and inserting “through the Office of
23 Partnership and Engagement”; and

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

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.

1 “(O) The Office of the Citizenship and Im-
2 migration Services Ombudsman.

3 “(P) The Office of Partnership and En-
4 gagement.

5 “(Q) The Countering Weapons of Mass
6 Destruction Office.

7 “(2) FUNCTIONS.—The Secretary, acting
8 through the appropriate official of the Headquarters,
9 shall—

10 “(A) establish an overall strategy to suc-
11 cessfully further the mission of the Department;

12 “(B) establish initiatives that improve De-
13 partment-wide operational performance;

14 “(C) establish mechanisms to—

15 “(i) ensure that components of the
16 Department comply with Department poli-
17 cies and fully implement the strategies and
18 initiatives of the Secretary; and

19 “(ii) require the head of each compo-
20 nent of the Department and component
21 chief officers to comply with such policies
22 and implement such strategies and initia-
23 tives;

1 “(D) establish annual operational and
2 management objectives to evaluate the perform-
3 ance of the Department;

4 “(E) ensure that the Department success-
5 fully meets operational and management per-
6 formance objectives through conducting over-
7 sight of component agencies;

8 “(F) ensure that the strategies, priorities,
9 investments, and workforce of Department com-
10 ponents align with Department objectives;

11 “(G) establish and implement policies re-
12 lated to Department ethics and compliance
13 standards;

14 “(H) establish and implement, in consulta-
15 tion with the Office of Civil Rights and Civil
16 Liberties, policies which preserve individual lib-
17 erty, fairness, and equality under the law;

18 “(I) manage and encourage shared services
19 across Department components;

20 “(J) lead and coordinate interaction with
21 Congress and other external organizations; and

22 “(K) carry out other such functions as the
23 Secretary determines are appropriate.”.

1 **SEC. 103. REPEAL OF DIRECTOR OF SHARED SERVICES AND**
2 **OFFICE OF COUNTERNARCOTICS ENFORCE-**
3 **MENT OF DEPARTMENT OF HOMELAND SECU-**
4 **RITY.**

5 (a) ABOLISHMENT OF DIRECTOR OF SHARED SERV-
6 ICES.—

7 (1) ABOLISHMENT.—The position of Director of
8 Shared Services of the Department of Homeland Se-
9 curity is abolished.

10 (2) CONFORMING AMENDMENT.—The Home-
11 land Security Act of 2002 is amended by striking
12 section 475 (6 U.S.C. 295).

13 (3) CLERICAL AMENDMENT.—The table of con-
14 tents in section 1(b) of such Act is amended by
15 striking the item relating to section 475.

16 (b) ABOLISHMENT OF THE OFFICE OF COUNTER-
17 NARCOTICS ENFORCEMENT.—

18 (1) ABOLISHMENT.—The Office of Counter-
19 narcotics Enforcement is abolished.

20 (2) CONFORMING AMENDMENTS.—The Home-
21 land Security Act of 2002 is amended—

22 (A) in subparagraph (B) of section
23 843(b)(1) (6 U.S.C. 413(b)(1)), by striking
24 “by—” and all that follows through the end of
25 that subparagraph and inserting “by the Sec-
26 retary; and”; and

1 (B) by striking section 878 (6 U.S.C.
2 112).

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

6 **SEC. 104. RESPONSIBILITIES AND FUNCTIONS OF CHIEF**
7 **PRIVACY OFFICER.**

8 (a) IN GENERAL.—Section 222 of the Homeland Se-
9 curity Act of 2002 (6 U.S.C. 142) is amended—

10 (1) in subsection (a)—

11 (A) in the matter preceding paragraph
12 (1)—

13 (i) by inserting “to be the Chief Pri-
14 vacy Officer of the Department and, if the
15 Secretary so appoints, the Chief Freedom
16 of Information Act (FOIA) Officer,” after
17 “in the Department,”; and

18 (ii) by striking “to the Secretary, to
19 assume primary responsibility for privacy
20 policy” and inserting “to the Secretary.
21 Such official shall be deemed the equiva-
22 lent of an Assistant Secretary, and shall
23 assume primary responsibility for privacy
24 policy and, if determined appropriate by

1 the Secretary, FOIA policy, of the Depart-
2 ment”;

3 (B) in paragraph (5)(B), by striking
4 “and” at the end; and

5 (C) by striking paragraph (6) and insert-
6 ing the following new paragraphs:

7 “(6) developing guidance and recommendations
8 to assist components of the Department in devel-
9 oping privacy policies and practices;

10 “(7) establishing a mechanism to ensure such
11 components are in compliance with Federal, regu-
12 latory, statutory, and Department privacy require-
13 ments, mandates, directives, and policies;

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

18 “(9) working with components and offices of
19 the Department to ensure that policy development,
20 information sharing, and information management
21 activities incorporate disclosure considerations and
22 privacy protections;

23 “(10) serving as the Chief FOIA Officer of the
24 Department for purposes of subsection (j) of section
25 552 of title 5, United States Code (popularly known

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

3 “(11) developing guidance on procedures to be
4 followed by individuals making requests for informa-
5 tion under such section 552;

6 “(12) overseeing hiring of FOIA officers and
7 the management and processing of requests for in-
8 formation under such section 552 within Depart-
9 ment Headquarters and relevant Department compo-
10 nent offices;

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

15 “(14) preparing an annual report to Congress
16 that includes a description of—

17 “(A) the activities of the Department that
18 affect privacy during the fiscal year covered by
19 the report, including complaints of privacy vio-
20 lations, implementation of section 552a of title
21 5, United States Code (popularly known as the
22 Privacy Act of 1974), internal controls, and
23 other matters; and

24 “(B) insignificant programs implemented
25 or revised in the Department during the fiscal

1 year covered by the report, the number of pro-
2 grams that the Chief Privacy Officer has evalu-
3 ated to ensure that privacy protections are con-
4 sidered and implemented, the number of pro-
5 grams reviewed that effectively implemented
6 privacy protections, and an explanation of why
7 any new programs did not effectively implement
8 privacy protections;

9 “(15) issuing guidance to relevant Department
10 component offices to ensure uniform disclosure poli-
11 cies and processes to administer such section 552;
12 and

13 “(16) carrying out such other responsibilities as
14 the Secretary determines are appropriate, consistent
15 with this section.”; and

16 (2) by adding at the end the following new sub-
17 sections:

18 “(f) REASSIGNMENT OF FUNCTIONS.—Notwith-
19 standing any requirement under this section, the Sec-
20 retary may reassign the functions related to managing and
21 processing requests for information under section 552 of
22 title 5, United States Code, to another officer within the
23 Department, consistent with requirements of such section.

24 “(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:

1 “(A) The development of guidance for uni-
2 form disclosure policies and processes, in ac-
3 cordance with paragraph (15) of subsection (a).

4 “(B) Ways to reduce unnecessary
5 redundancies that may undermine the respon-
6 sive and efficient processing of requests for in-
7 formation under such section 552.”.

8 **SEC. 105. UNMANNED AIRCRAFT SYSTEMS COUNTER-**
9 **MEASURES COORDINATOR.**

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

13 **“SEC. 321. COUNTERING UNMANNED AIRCRAFT SYSTEMS**
14 **COORDINATOR.**

15 “(a) COORDINATOR.—The Secretary shall designate
16 a senior official of the Office of Strategy, Policy and Plans
17 of the Department as the Countering Unmanned Aircraft
18 Systems (UAS) Coordinator (in this section referred to as
19 the ‘Coordinator’) to coordinate with relevant Department
20 offices and components, including the Office for Civil
21 Rights and Civil Liberties and the Privacy Office and
22 other relevant Federal agencies, as appropriate, on the de-
23 velopment of policies and plans to counter threats associ-
24 ated with UAS in accordance with section 210G, including
25 the following:

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

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

6 “(3) Coordinate with the relevant components
7 and offices of the Department, including the Office
8 of Intelligence and Analysis, to ensure the sharing
9 and retention of information, guidance, and intel-
10 ligence relating to countering UAS threats, counter
11 UAS threat assessment, and counter UAS tech-
12 nology.

13 “(4) Serving as the Department point of con-
14 tact for Federal, State, local, and Tribal law en-
15 forcement entities and the private sector regarding
16 the Department’s activities related to countering
17 UAS.

18 “(5) Carrying out other related UAS authori-
19 ties and activities under such section 210G, as di-
20 rected by the Secretary.

21 “(b) COORDINATION WITH APPLICABLE FEDERAL
22 LAWS.—The Coordinator shall, in addition to other as-
23 signed duties, coordinate with relevant Department offices
24 and components and other relevant Federal agencies, as
25 appropriate, to ensure testing, evaluation, or deployment

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

3 “(c) COORDINATION WITH PRIVATE SECTOR.—The
4 Coordinator shall, working with the Office of Partnership
5 and Engagement and other relevant Department offices
6 and components, or other Federal agencies, as appro-
7 priate, serve as the principal Department official respon-
8 sible for disseminating to the private sector information
9 regarding counter UAS technology, particularly informa-
10 tion regarding instances in which counter UAS technology
11 may impact lawful private sector services or systems.

12 “(d) TERMINATION.—The authority to carry out this
13 section terminates on the date specified in section
14 210G(i).”.

15 (b) CLERICAL AMENDMENT.—The table of contents
16 in section 1(b) of the Homeland Security Act of 2002 is
17 amended by inserting after the item relating to section
18 320 the following new item:

“Sec. 321. Countering Unmanned Aircraft Systems Coordinator.”.

19 **SEC. 106. RESPONSIBILITIES OF CHIEF FINANCIAL OFFI-**
20 **CER.**

21 (a) IN GENERAL.—Section 702 of the Homeland Se-
22 curity Act of 2002 (6 U.S.C. 342) is amended—

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

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

3 “(b) RESPONSIBILITIES.—In carrying out the re-
4 sponsibilities, authorities, and functions specified in sec-
5 tion 902 of title 31, United States Code, the Chief Finan-
6 cial Officer shall—

7 “(1) oversee Department budget formulation
8 and execution;

9 “(2) lead and provide guidance on performance-
10 based budgeting practices for the Department to en-
11 sure that the Department and its components are
12 meeting missions and goals;

13 “(3) lead cost-estimating practices for the De-
14 partment, including the development of policies on
15 cost estimating and approval of life cycle cost esti-
16 mates;

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

22 “(5) develop financial management policy for
23 the Department and oversee the implementation of
24 such policy, including the establishment of effective

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

3 “(6) provide guidance for and over financial
4 system modernization efforts throughout the Depart-
5 ment;

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

9 “(8) oversee the costs of acquisition programs
10 and related activities to ensure that actual and
11 planned costs are in accordance with budget esti-
12 mates and are affordable, or can be adequately fund-
13 ed, over the lifecycle of such programs and activities;

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

17 “(10) track, approve, oversee, and make public
18 information on expenditures by components of the
19 Department for conferences, as appropriate, includ-
20 ing by requiring each component to—

21 “(A) report to the Inspector General of the
22 Department the expenditures by such compo-
23 nent for each conference hosted or attended by
24 Department employees for which the total ex-
25 penditures of the Department exceed \$20,000,

1 within 15 days after the date of the conference;
2 and

3 “(B) with respect to such expenditures,
4 provide to the Inspector General—

5 “(i) the information described in sub-
6 sections (a), (b), and (c) of section 739 of
7 title VII of division E of the Consolidated
8 and Further Continuing Appropriations
9 Act, 2015 (Public Law 113-235); and

10 “(ii) documentation of such expendi-
11 tures.”.

12 (b) **RULE OF CONSTRUCTION.**—Nothing in the
13 amendment made by this section may be construed as al-
14 tering or amending the responsibilities, authorities, and
15 functions of the Chief Financial Officer of the Department
16 of Homeland Security under section 902 of title 31,
17 United States Code.

18 **SEC. 107. CHIEF INFORMATION OFFICER.**

19 (a) **IN GENERAL.**—Section 703 of the Homeland Se-
20 curity Act of 2002 (6 U.S.C. 343) is amended—

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

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

3 (2) by redesignating subsection (b) as sub-
4 section (d); and

5 (3) by inserting after subsection (a) the fol-
6 lowing new subsections:

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

13 “(1) advise and assist the Secretary, heads of
14 the components of the Department, and other senior
15 officers in carrying out the responsibilities of the
16 Department for all activities relating to the budgets,
17 programs, security, and operations of the informa-
18 tion technology functions of the Department;

19 “(2) to the extent delegated by the Secretary,
20 exercise leadership and authority over Department
21 information technology management and establish
22 the information technology priorities, policies, proc-
23 esses, standards, guidelines, and procedures of the
24 Department to ensure interoperability and standard-
25 ization 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-

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

3 “(1) the budget of the Department aligns with
4 priorities specified in the information technology
5 strategic plan;

6 “(2) the information technology strategic plan
7 informs the budget process of the Department;

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

11 “(4) the Department has identified and ad-
12 dressed skills gaps needed to implement the informa-
13 tion technology strategic plan; and

14 “(5) unnecessary duplicate information tech-
15 nology within and across the components of the De-
16 partment has been eliminated.”.

17 (b) SOFTWARE LICENSING.—

18 (1) SOFTWARE INVENTORY.—Not later than
19 180 days after the date of the enactment of this Act
20 and every two years thereafter until 2024, the Chief
21 Information Officer of the Department of Homeland
22 Security, in consultation with Department compo-
23 nent chief information officers, shall—

24 (A) conduct a Department-wide inventory
25 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

1 the inventory conducted under paragraph (1) that
2 the number of software licenses held by the Depart-
3 ment and the components of the Department exceed
4 the needs of the Department, not later than 90 days
5 after the date on which the inventory is completed,
6 the Secretary of Homeland Security shall establish a
7 plan for reducing the number of such software li-
8 censes to meet needs of the Department.

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

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

19 (B) EXCEPTION.—The Chief Information
20 Officer may authorize the purchase of addi-
21 tional licenses and amend the number of needed
22 licenses as necessary.

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

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

3 (d) COMPLETION OF FIRST DEFINITION OF CAPA-
4 BILITIES.—Not later than one year after the date of the
5 enactment of this Act, the Chief Information Officer shall
6 complete the first information technology strategic plan
7 required under subsection (c) of section 701 of the Home-
8 land Security Act of 2002, as added by subsection (a) of
9 this section.

10 **SEC. 108. QUADRENNIAL HOMELAND SECURITY REVIEW.**

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

13 (1) in subsection (a)(3)—

14 (A) in subparagraph (B), by striking
15 “and” at the end;

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

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

20 “(C) representatives from appropriate ad-
21 visory committees established pursuant to sec-
22 tion 871, including the Homeland Security Ad-
23 visory Council and the Homeland Security
24 Science and Technology Advisory Committee, or
25 otherwise established, including the Aviation

1 Security Advisory Committee established pursu-
2 ant to section 44946 of title 49, United States
3 Code; and”;

4 (2) in subsection (b)—

5 (A) in paragraph (2), by inserting before
6 the semicolon at the end the following: “based
7 on the risk assessment required pursuant to
8 subsection (c)(2)(B)”;

9 (B) in paragraph (3)—

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

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

14 (C) in paragraph (4)—

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

17 (ii) by striking “budget plan required
18 to provide sufficient resources to success-
19 fully” and inserting “resources required
20 to”; and

21 (iii) by striking the semicolon at the
22 end and inserting “, including any re-
23 sources identified from redundant, waste-
24 ful, or unnecessary capabilities and capac-
25 ities that can be redirected to better sup-

1 port other existing capabilities and capacities,
2 ities, as the case may be; and”;

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

5 (E) by striking paragraph (6);

6 (3) in subsection (c)—

7 (A) in paragraph (1), by striking “December
8 ber 31 of the year” and inserting “60 days
9 after the date of the submittal of the President’s
10 budget for the fiscal year after the fiscal
11 year”;

12 (B) in paragraph (2)—

13 (i) in subparagraph (B), by striking
14 “description of the threats to” and inserting
15 “risk assessment of”;

16 (ii) in subparagraph (C), by inserting
17 “, as required under subsection (b)(2)” before
18 the semicolon at the end;

19 (iii) in subparagraph (D)—

20 (I) by inserting “to the extent
21 practicable,” before “a description”;
22 and

23 (II) by striking “budget plan”
24 and inserting “resources required”;

25 (iv) in subparagraph (F)—

1 (I) by inserting “to the extent
2 practicable,” before “a discussion”;
3 and

4 (II) by striking “the status of”;
5 (v) in subparagraph (G)—

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

8 (II) by striking “the status of”;

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

11 (IV) by inserting “and” after the
12 semicolon at the end;

13 (vi) by striking subparagraph (H);

14 and

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

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

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

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

1 of the Senate information on the degree to which the find-
2 ings and recommendations developed in the quadrennial
3 homeland security review covered by the report were inte-
4 grated into the acquisition strategy and expenditure plans
5 for the Department.”.

6 (b) EFFECTIVE DATE.—The amendments made by
7 this section shall apply with respect to a quadrennial
8 homeland security review conducted after December 31,
9 2020.

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

11 (a) IN GENERAL.—Section 709 of the Homeland Se-
12 curity Act of 2002 (6 U.S.C. 349) is amended—

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

16 “(1) The Office of International Affairs.

17 “(2) The Office of Cyber Policy.

18 “(3) The Office of Strategy, Planning, Analysis,
19 and Risk.

20 “(4) The Office of Threat Prevention and Secu-
21 rity Policy.

22 “(5) The Office of Border, Immigration, and
23 Trade Policy.”.

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

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

3 “(e) ASSISTANT SECRETARY FOR INTERNATIONAL
4 AFFAIRS.—The Office of International Affairs shall be led
5 by an Assistant Secretary for International Affairs ap-
6 pointed by the Secretary. The Assistant Secretary shall—

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

12 “(2) advise, inform, and assist the Secretary
13 with respect to the development and implementation
14 of the policy priorities of the Department, including
15 strategic priorities for the deployment of assets, in-
16 cluding personnel, outside the United States;

17 “(3) develop, in consultation with the Under
18 Secretary for Management, guidance for selecting,
19 assigning, training, and monitoring overseas deploy-
20 ments of Department personnel, including minimum
21 standards for pre-deployment training;

22 “(4) maintain awareness regarding the inter-
23 national travel of senior officers of the Department
24 and their intent to pursue negotiations with foreign

1 government officials, and review resulting draft
2 agreements; and

3 “(5) perform such other functions as are estab-
4 lished by law or delegated by the Under Secretary
5 for Policy.”.

6 (b) ABOLISHMENT OF OFFICE OF INTERNATIONAL
7 AFFAIRS.—

8 (1) IN GENERAL.—The Office of International
9 Affairs within the Office of the Secretary of Home-
10 land Security is abolished.

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

19 (3) CONFORMING AMENDMENT.—The Home-
20 land Security Act of 2002 is amended by striking
21 section 879 (6 U.S.C. 459).

22 (4) CLERICAL AMENDMENT.—The table of con-
23 tents in section 1(b) of such Act is amended by
24 striking the item relating to section 879.

1 (c) CONFORMING AMENDMENTS RELATING TO AS-
2 SISTANT SECRETARIES.—Subsection (a) of section 103 of
3 the Homeland Security Act of 2002 (6 U.S.C. 113) is
4 amended—

5 (1) in the subsection heading, by inserting “;
6 Assistant Secretaries and Other Officers” after
7 “Under Secretaries”;

8 (2) in paragraph (1), by amending subpara-
9 graph (I) to read as follows:

10 “(I) An Administrator of the Transpor-
11 tation Security Administration.”;

12 (3) by amending paragraph (2) to read as fol-
13 lows:

14 “(2) ASSISTANT SECRETARIES.—The following
15 Assistant Secretaries shall be appointed by the
16 President or the Secretary, as the case may be, with-
17 out the advice and consent of the Senate:

18 “(A) PRESIDENTIAL APPOINTMENTS.—The
19 Department shall have the following officials
20 appointed by the President:

21 “(i) The Assistant Secretary for the
22 Countering Weapons of Mass Destruction
23 Office.

24 “(ii) The Assistant Secretary for Pub-
25 lic 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

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

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

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

11 (1) in paragraph (2), by striking “and” at the
12 end;

13 (2) in paragraph (3), by striking the period at
14 the end and inserting “; and”; and

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

17 “(4) shall establish a Homeland Security Advi-
18 sory Council to provide advice and recommendations
19 on homeland security-related matters, including ad-
20 vice with respect to the preparation of the Quadren-
21 nial Homeland Security Review.”.

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

1 (f) DUPLICATION REVIEW.—

2 (1) REVIEW REQUIRED.—Not later than one
3 year after the date of the enactment of this Act, the
4 Secretary of Homeland Security shall complete a re-
5 view of the functions and responsibilities of each De-
6 partment of Homeland Security component respon-
7 sible for international affairs to identify and elimi-
8 nate areas of unnecessary duplication.

9 (2) SUBMISSION TO CONGRESS.—Not later than
10 60 days after the completion of the review required
11 under paragraph (1), the Secretary shall provide the
12 results of the review to the Committee on Homeland
13 Security of the House of Representatives and the
14 Committee on Homeland Security and Governmental
15 Affairs of the Senate.

16 (3) ACTION PLAN.—Not later than one year
17 after the date of the enactment of this Act, the Sec-
18 retary shall submit to the congressional homeland
19 security committees an action plan, including correc-
20 tive steps and an estimated date of completion, to
21 address areas of duplication, fragmentation, and
22 overlap and opportunities for cost savings and rev-
23 enue enhancement, as identified by the Government
24 Accountability Office based on the annual report of
25 the Government Accountability Office entitled “Ad-

1 ditional Opportunities to Reduce Fragmentation,
2 Overlap, and Duplication and Achieve Other Finan-
3 cial Benefits”.

4 **SEC. 110. CHIEF PROCUREMENT OFFICER.**

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

8 **“SEC. 711. CHIEF PROCUREMENT OFFICER.**

9 “(a) IN GENERAL.—There is in the Department a
10 Chief Procurement Officer, who shall serve as a senior
11 business advisor to agency officials on procurement-re-
12 lated matters and report directly to the Under Secretary
13 for Management. The Chief Procurement Officer is the
14 senior procurement executive for purposes of subsection
15 (c) of section 1702 of title 41, United States Code, and
16 shall perform procurement functions as specified in such
17 subsection.

18 “(b) RESPONSIBILITIES.—The Chief Procurement
19 Officer shall—

20 “(1) delegate or retain contracting authority, as
21 appropriate;

22 “(2) issue procurement policies and oversee the
23 heads of contracting activity of the Department to
24 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

1 vulnerabilities in the supply chain for all Depart-
2 ment purchases;

3 “(10) ensure that a fair proportion of the value
4 of Federal contracts and subcontracts are awarded
5 to small businesses (in accordance with the procure-
6 ment contract goals under section 15(g) of the Small
7 Business Act (15 U.S.C. 644(g)), maximize opportu-
8 nities for small business participation in such con-
9 tracts, and ensure, to the extent practicable, small
10 businesses that achieve qualified vendor status for
11 security-related technologies are provided an oppor-
12 tunity to compete for contracts for such technology;

13 “(11) conduct oversight of implementation of
14 administrative agreements to resolve suspension or
15 debarment proceedings; and

16 “(12) carry out any other procurement duties
17 that the Under Secretary for Management may des-
18 ignate.

19 “(c) HEAD OF CONTRACTING ACTIVITY DEFINED.—
20 In this section the term ‘head of contracting activity’
21 means an official responsible for the creation, manage-
22 ment, and oversight of a team of procurement profes-
23 sionals properly trained, certified, and warranted to ac-
24 complish the acquisition of products and services on behalf
25 of the designated components, offices, and organizations

1 of the Department, and as authorized, other government
2 entities.”.

3 (b) CLERICAL AMENDMENT.—The table of contents
4 in section 1(b) of the Homeland Security Act of 2002, is
5 amended by inserting after the item relating to section
6 710 the following new item:

“Sec. 711. Chief Procurement Officer.”.

7 **SEC. 111. CHIEF SECURITY OFFICER.**

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

12 **“SEC. 712. CHIEF SECURITY OFFICER.**

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

16 “(b) RESPONSIBILITIES.—The Chief Security Officer
17 shall—

18 “(1) develop and implement the security poli-
19 cies, programs, and standards of the Department;

20 “(2) identify training and provide education to
21 Department personnel on security-related matters;
22 and

23 “(3) provide support to Department compo-
24 nents on security-related matters.”.

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

“Sec. 712. Chief Security Officer.”.

5 **SEC. 112. OFFICE OF PARTNERSHIP AND ENGAGEMENT.**

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

9 **“SEC. 801. OFFICE OF PARTNERSHIP AND ENGAGEMENT.**

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

13 “(b) RESPONSIBILITIES.—The Assistant Secretary
14 shall—

15 “(1) lead the efforts of the Department to in-
16 corporate external feedback from stakeholders into
17 policy and strategic planning efforts, as appropriate,
18 in consultation with the Office for Civil Rights and
19 Civil Liberties;

20 “(2) oversee and support the activities con-
21 ducted under section 2006(b);

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

1 tor to enhance the primary mission of the Depart-
2 ment to protect the homeland;

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

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

9 “(6) perform such other functions as are estab-
10 lished by law or delegated by the Secretary.”.

11 (b) OFFICE FOR STATE AND LOCAL LAW ENFORCE-
12 MENT.—Paragraph (1) of section 2006(b) of the Home-
13 land Security Act of 2002 (6 U.S.C. 607(b)) is amended
14 by striking “Policy Directorate” and inserting “Office of
15 Partnership and Engagement”.

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

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

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

1 Office of Partnership and Engagement under section
2 801 of the Homeland Security Act of 2002, as
3 amended by this section.

4 (d) ABOLISHMENT OF SPECIAL ASSISTANT TO SEC-
5 RETARY OF HOMELAND SECURITY.—

6 (1) IN GENERAL.—The position of Special As-
7 sistant to the Secretary of Homeland Security au-
8 thorized under section 102(f) of the Homeland Secu-
9 rity Act of 2002 (6 U.S.C. 112(f)), as in effect on
10 the day before the date of the enactment of this Act,
11 is abolished.

12 (2) TRANSFER OF FUNCTIONS AND ASSETS.—
13 The functions authorized to be performed by such
14 Special Assistant to the Secretary as of the day be-
15 fore such date of enactment, and the assets and per-
16 sonnel associated with such functions, are trans-
17 ferred to the head of the Office of Partnership and
18 Engagement under section 801 of the Homeland Se-
19 curity Act of 2002, as amended by this section.

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

23 (A) striking subsection (f); and

24 (B) redesignating subsection (g) as sub-
25 section (f).

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

“Sec. 801. Office of Partnership and Engagement.”.

4 **SEC. 113. DEPARTMENT OF HOMELAND SECURITY ROTA-**
5 **TION PROGRAM.**

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

9 (1) by striking “(a) ESTABLISHMENT—.”;

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

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

14 (A) by striking “Not later than 180 days
15 after the date of enactment of this section, the”
16 and inserting “The”; and

17 (B) by striking “for employees of the De-
18 partment” and inserting “for certain personnel
19 within the Department”;

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

21 (A) by redesignating subparagraphs (A)
22 through (G) as paragraphs (3) through (9), re-
23 spectively, and adjusting the margins accord-
24 ingly;

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

3 “(1) seek to foster greater departmental inte-
4 gration and unity of effort;

5 “(2) seek to help enhance the knowledge, skills,
6 and abilities of participating personnel with respect
7 to the programs, policies, and activities of the De-
8 partment;”;

9 (C) in paragraph (4), as so redesignated,
10 by striking “middle and senior level”; and

11 (D) in paragraph (7), as so redesignated,
12 by inserting before “invigorate” the following:
13 “seek to improve morale and retention through-
14 out the Department and”;

15 (5) in subsection (c), as redesignated by para-
16 graph (2)—

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

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

21 (i) by striking clause (iii); and

22 (ii) by redesignating clauses (i), (ii),
23 and (iv) through (viii) as subparagraphs
24 (A) through (G), respectively, and adjust-

25 ing the margins accordingly;

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

4 (7) by inserting after subsection (c) the fol-
5 lowing new subsection:

6 “(d) ADMINISTRATIVE MATTERS.—In carrying out
7 the Rotation Program the Secretary shall—

8 “(1) before selecting employees for participation
9 in the Rotation Program, disseminate information
10 broadly within the Department about the availability
11 of the Rotation Program, qualifications for partici-
12 pation in the Rotation Program, including full-time
13 employment within the employing component or of-
14 fice not less than one year, and the general provi-
15 sions of the Rotation Program;

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

18 “(A) is nominated by the head of the com-
19 ponent or office employing the employee; and

20 “(B) is selected by the Secretary, or the
21 Secretary’s designee, solely on the basis of rel-
22 ative ability, knowledge, and skills, after fair
23 and open competition that assures that all can-
24 didates receive equal opportunity;

1 “(3) ensure that each employee participating in
2 the Rotation Program shall be entitled to return,
3 within a reasonable period of time after the end of
4 the period of participation, to the position held by
5 the employee, or a corresponding or higher position,
6 in the component or office that employed the em-
7 ployee prior to the participation of the employee in
8 the Rotation Program;

9 “(4) require that the rights that would be avail-
10 able to the employee if the employee were detailed
11 from the employing component or office to another
12 Federal agency or office remain available to the em-
13 ployee during the employee participation in the Ro-
14 tation Program; and

15 “(5) require that, during the period of partici-
16 pation by an employee in the Rotation Program, per-
17 formance evaluations for the employee—

18 “(A) shall be conducted by officials in the
19 office or component employing the employee
20 with input from the supervisors of the employee
21 at the component or office in which the em-
22 ployee is placed during that period; and

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

1 fice or component employing the employee.”;

2 and

3 (8) by adding at the end the following new sub-

4 section:

5 “(g) INTELLIGENCE ROTATIONAL ASSIGNMENT PRO-

6 GRAM.—

7 “(1) ESTABLISHMENT.—The Secretary shall es-
8 tablish an Intelligence Rotational Assignment Pro-
9 gram as part of the Rotation Program under sub-
10 section (a).

11 “(2) ADMINISTRATION.—The Chief Human
12 Capital Officer, in conjunction with the Chief Intel-
13 ligence Officer, shall administer the Intelligence Ro-
14 tational Assignment Program established pursuant
15 to paragraph (1).

16 “(3) ELIGIBILITY.—The Intelligence Rotational
17 Assignment Program established pursuant to para-
18 graph (1) shall be open to employees serving in ex-
19 isting analyst positions within the Department’s In-
20 telligence Enterprise and other Department employ-
21 ees as determined appropriate by the Chief Human
22 Capital Officer and the Chief Intelligence Officer.

23 “(4) COORDINATION.—The responsibilities
24 specified in subsection (c)(2) that apply to the Rota-
25 tion Program under such subsection shall, as appli-

1 cable, also apply to the Intelligence Rotational As-
2 signment Program under this subsection.”.

3 (b) CONGRESSIONAL NOTIFICATION AND OVER-
4 SIGHT.—Not later than 120 days after the date of the en-
5 actment of this Act, the Secretary of Homeland Security
6 shall provide to the Committee on Homeland Security and
7 the Permanent Select Committee on Intelligence of the
8 House of Representatives and the Committee on Home-
9 land Security and Governmental Affairs of the Senate in-
10 formation about the status of the Homeland Security Ro-
11 tation Program authorized by section 844 of the Home-
12 land Security Act of 2002, as amended by subsection (a)
13 of this section.

14 **SEC. 114. ANNUAL SUBMISSION TO CONGRESS OF INFOR-**
15 **MATION REGARDING REPROGRAMMING OR**
16 **TRANSFER OF DEPARTMENT OF HOMELAND**
17 **SECURITY RESOURCES TO RESPOND TO**
18 **OPERATIONAL SURGES.**

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

1 **“SEC. 713. ANNUAL SUBMISSION TO CONGRESS OF INFOR-**
2 **MATION ON REPROGRAMMING OR TRANS-**
3 **FERS OF FUNDS TO RESPOND TO OPER-**
4 **ATIONAL SURGES.**

5 “For each fiscal year until fiscal year 2023, the Sec-
6 retary of Homeland Security shall provide to the Com-
7 mittee on Homeland Security of the House of Representa-
8 tives and the Committee on Homeland Security and Gov-
9 ernmental Affairs of the Senate, together with the annual
10 budget request for the Department, information on—

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

16 “(2) any circumstance in which any limitation
17 on the transfer or reprogramming of funds affected
18 the ability of the Secretary to address such unfore-
19 seen costs.”.

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

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

1 **SEC. 115. OVERSEAS PERSONNEL BRIEFING.**

2 (a) BRIEFING REQUIRED.—

3 (1) IN GENERAL.—Not later than 90 days after
4 the date of the enactment of this Act and every 180
5 days thereafter, the Secretary of Homeland Security
6 shall provide to the Committee on Homeland Security
7 of the House of Representatives and the Committee
8 on Homeland Security and Governmental Affairs
9 of the Senate a briefing regarding Department
10 of Homeland Security personnel with primary duties
11 that take place outside of the United States.

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

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

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

24 (C) Information related to any risk mitigation
25 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.

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

3 (J) The status of efforts (beginning with
4 the second briefing required under this sub-
5 section) to implement the enhancement plan
6 under subsection (b).

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

11 (b) OVERSEAS PERSONNEL ENHANCEMENT PLAN.—

12 (1) IN GENERAL.—Not later than 90 days after
13 the first briefing required under subsection (a), the
14 Secretary shall submit to the Committee on Home-
15 land Security of the House and the Committee on
16 Homeland Security and Governmental Affairs of the
17 Senate a plan to enhance the effectiveness of De-
18 partment of Homeland Security personnel at foreign
19 locations.

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

22 (A) improve efforts of Department of
23 Homeland Security personnel at foreign loca-
24 tions, as necessary, for purposes of providing
25 foreign partner capacity development and fur-

1 thering the Department’s counterterrorism mis-
2 sion;

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

6 (C) enhance collaboration among Depart-
7 ment personnel at foreign locations, other Fed-
8 eral personnel at foreign locations, and foreign
9 partners;

10 (D) improve the communication of counter-
11 terrorism information between Department per-
12 sonnel at foreign locations and Department en-
13 tities in the United States, including to address
14 technical, resource, and administrative chal-
15 lenges; and

16 (E) maintain practices to guard against
17 counter-espionage threats associated with De-
18 partment personnel.

19 **Subtitle B—Acquisition Reform**

20 **SEC. 121. ACQUISITION REVIEW BOARD.**

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

1 **“SEC. 836. ACQUISITION REVIEW BOARD.**

2 “(a) IN GENERAL.—The Secretary shall establish an
3 Acquisition Review Board (in this section referred to as
4 the ‘Board’) to—

5 “(1) strengthen accountability and uniformity
6 within the Department acquisition review process;

7 “(2) review major acquisition programs; and

8 “(3) review the use of best practices.

9 “(b) COMPOSITION.—

10 “(1) CHAIR.—The Under Secretary for Man-
11 agement shall serve as chair of the Board.

12 “(2) PARTICIPATION.— The Secretary shall en-
13 sure participation by other relevant Department offi-
14 cials with responsibilities related to acquisitions as
15 permanent members of the Board.

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

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

25 “(1) a major acquisition program—

1 “(A) requires authorization to proceed
2 from one acquisition decision event to another
3 throughout the acquisition life cycle;

4 “(B) is in breach of its approved require-
5 ments; or

6 “(C) requires additional review, as deter-
7 mined by the Under Secretary for Management;
8 or

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

12 “(d) RESPONSIBILITIES.—The responsibilities of the
13 Board are as follows:

14 “(1) Determine whether a proposed acquisition
15 has met the requirements of key phases of the acqui-
16 sition life cycle framework and is able to proceed to
17 the next phase and eventual full production and de-
18 ployment.

19 “(2) Oversee whether a proposed acquisition’s
20 business strategy, resources, management, and ac-
21 countability is executable and is aligned to strategic
22 initiatives.

23 “(3) Support the person with acquisition deci-
24 sion authority for an acquisition in determining the

1 appropriate direction for such acquisition at key ac-
2 quisition decision events.

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

7 “(5) Review the acquisition documents of each
8 major acquisition program, including the acquisition
9 program baseline and documentation reflecting con-
10 sideration of tradeoffs among cost, schedule, and
11 performance objectives, to ensure the reliability of
12 underlying data.

13 “(6) Ensure that practices are adopted and im-
14 plemented to require consideration of trade-offs
15 among cost, schedule, and performance objectives as
16 part of the process for developing requirements for
17 major acquisition programs prior to the initiation of
18 the second acquisition decision event, including, at a
19 minimum, the following practices:

20 “(A) Department officials responsible for
21 acquisition, budget, and cost estimating func-
22 tions are provided with the appropriate oppor-
23 tunity to develop estimates and raise cost and
24 schedule matters before performance objectives
25 are established for capabilities when feasible.

1 “(B) Full consideration is given to possible
2 trade-offs among cost, schedule, and perform-
3 ance objectives for each alternative.

4 “(e) ACQUISITION PROGRAM BASELINE REPORT RE-
5 QUIREMENT.—If the person exercising acquisition decision
6 authority over a major acquisition program approves such
7 program to proceed into the planning phase before such
8 program has a Department-approved acquisition program
9 baseline, the Under Secretary for Management shall cre-
10 ate and approve an acquisition program baseline report
11 regarding such approval, and the Secretary shall—

12 “(1) within 7 days after an acquisition decision
13 memorandum is signed, notify in writing the Com-
14 mittee on Homeland Security of the House of Rep-
15 resentatives and the Committee on Homeland Secu-
16 rity and Governmental Affairs of the Senate of such
17 decision; and

18 “(2) within 60 days after the acquisition deci-
19 sion memorandum is signed, submit to such commit-
20 tees a written explanation of the rationale for such
21 decision and a plan of action to address acquisition
22 program baseline requirements for such program.

23 “(f) REPORT.—The Under Secretary for Manage-
24 ment shall provide information to the Committee on
25 Homeland Security of the House of Representatives and

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

5 “(1) For each meeting of the Board, any acqui-
6 sition decision memoranda.

7 “(2) Results of the systematic reviews con-
8 ducted pursuant to paragraph (4) of subsection (d).

9 “(3) Results of acquisition document reviews re-
10 quired pursuant to paragraph (5) of subsection (d).

11 “(4) Activities to ensure that practices are
12 adopted and implemented throughout the Depart-
13 ment pursuant to paragraph (6) of subsection (d).

14 “(g) DEFINITIONS.—In this section:

15 “(1) ACQUISITION.—The term ‘acquisition’ has
16 the meaning given such term in section 131 of title
17 41, United States Code.

18 “(2) ACQUISITION DECISION AUTHORITY.—The
19 term ‘acquisition decision authority’ means the au-
20 thority, held by the Secretary acting through the
21 Deputy Secretary or Under Secretary for Manage-
22 ment to—

23 “(A) ensure compliance with Federal law,
24 the Federal Acquisition Regulation, and De-
25 partment acquisition management directives;

1 “(B) review (including approving, pausing,
2 modifying, or cancelling) an acquisition pro-
3 gram through the life cycle of such program;

4 “(C) ensure that acquisition program man-
5 agers have the resources necessary to success-
6 fully execute an approved acquisition program;

7 “(D) ensure good acquisition program
8 management of cost, schedule, risk, and system
9 performance of the acquisition program at
10 issue, including assessing acquisition program
11 baseline breaches and directing any corrective
12 action for such breaches; and

13 “(E) ensure that acquisition program man-
14 agers, on an ongoing basis, monitor cost, sched-
15 ule, and performance against established base-
16 lines and use tools to assess risks to an acquisi-
17 tion program at all phases of the life cycle of
18 such program to avoid and mitigate acquisition
19 program baseline breaches.

20 “(3) ACQUISITION DECISION EVENT.—The term
21 ‘acquisition decision event’, with respect to an acqui-
22 sition program, means a predetermined point within
23 each of the acquisition phases at which the acquisi-
24 tion decision authority determines whether such ac-

1 quisition program shall proceed to the next acquisi-
2 tion phase.

3 “(4) ACQUISITION DECISION MEMORANDUM.—
4 The term ‘acquisition decision memorandum’, with
5 respect to an acquisition, means the official acquisi-
6 tion decision event record that includes a docu-
7 mented record of decisions, exit criteria, and as-
8 signed actions for such acquisition, as determined by
9 the person exercising acquisition decision authority
10 for such acquisition.

11 “(5) ACQUISITION PROGRAM.—The term ‘acqui-
12 sition program’ means the process by which the De-
13 partment acquires, with any appropriated amounts,
14 by contract for purchase or lease, property or serv-
15 ices (including construction) that support the mis-
16 sions and goals of the Department.

17 “(6) ACQUISITION PROGRAM BASELINE.—The
18 term ‘acquisition program baseline’, with respect to
19 an acquisition program, means a summary of the
20 cost, schedule, and performance parameters, ex-
21 pressed in standard, measurable, quantitative terms,
22 which must be met in order to accomplish the goals
23 of such program.

24 “(7) BEST PRACTICES.—The term ‘best prac-
25 tices’, with respect to acquisition, means a knowl-

1 edge-based approach to capability development that
2 includes—

3 “(A) identifying and validating needs;

4 “(B) assessing alternatives to select the
5 most appropriate solution;

6 “(C) clearly establishing well-defined re-
7 quirements;

8 “(D) developing realistic cost assessments
9 and schedules;

10 “(E) securing stable funding that matches
11 resources to requirements;

12 “(F) demonstrating technology, design,
13 and manufacturing maturity;

14 “(G) using milestones and exit criteria or
15 specific accomplishments that demonstrate
16 progress;

17 “(H) adopting and executing standardized
18 processes with known success across programs;

19 “(I) establishing an adequate workforce
20 that is qualified and sufficient to perform nec-
21 essary functions; and

22 “(J) integrating the capabilities described
23 in subparagraphs (A) through (I) into the De-
24 partment’s mission and business operations.

1 “(8) MAJOR ACQUISITION PROGRAM.—The term
2 ‘major acquisition program’ means a Department
3 acquisition program that is estimated by the Sec-
4 retary to require an eventual total expenditure of at
5 least \$300 million (based on fiscal year 2019 con-
6 stant dollars) over its life cycle cost.”.

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

 “Sec. 836. Acquisition Review Board.”.

11 **SEC. 122. ACQUISITION AUTHORITIES FOR UNDER SEC-**
12 **RETARY FOR MANAGEMENT OF THE DEPART-**
13 **MENT OF HOMELAND SECURITY.**

14 Section 701 of the Homeland Security Act of 2002
15 (6 U.S.C. 341) is amended by—

16 (1) redesignating subsection (d), the first sub-
17 section (e) (relating to the system for award man-
18 agement consultation), and the second subsection (e)
19 (relating to the definition of interoperable commu-
20 nications) as subsections (e), (f), and (g), respec-
21 tively; and

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

24 “(d) ACQUISITION AND RELATED RESPONSIBIL-
25 ITIES.—

1 “(1) IN GENERAL.—Notwithstanding section
2 1702(a) of title 41, United States Code, the Under
3 Secretary for Management is the Chief Acquisition
4 Officer of the Department. As Chief Acquisition Of-
5 ficer, the Under Secretary shall have the authorities
6 and perform the functions specified in such section
7 1702(b), and perform all other functions and re-
8 sponsibilities delegated by the Secretary or described
9 in this subsection.

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

16 “(A) Advising the Secretary regarding ac-
17 quisition management activities, taking into ac-
18 count risks of failure to achieve cost, schedule,
19 or performance parameters, to ensure that the
20 Department achieves its mission through the
21 adoption of widely accepted program manage-
22 ment best practices (as such term is defined in
23 section 836) and standards and, where appro-
24 priate, acquisition innovation best practices.

1 “(B) Leading the Department’s acquisition
2 oversight body, the Acquisition Review Board.

3 “(C) Exercising the acquisition decision
4 authority (as such term is defined in section
5 836) to approve, pause, modify (including the
6 rescission of approvals of program milestones),
7 or cancel major acquisition programs (as such
8 term is defined in section 836), unless the
9 Under Secretary delegates such authority to a
10 Component Acquisition Executive (as such term
11 is defined in section 836) pursuant to para-
12 graph (3).

13 “(D) Establishing policies for acquisition
14 that implement an approach that takes into ac-
15 count risks of failure to achieve cost, schedule,
16 or performance parameters that all components
17 of the Department shall comply with, including
18 outlining relevant authorities for program man-
19 agers to effectively manage acquisition pro-
20 grams (as such term is defined in section 836).

21 “(E) Ensuring that each major acquisition
22 program has a Department-approved acquisi-
23 tion program baseline (as such term is defined
24 in section 836), pursuant to the Department’s
25 acquisition management policy.

1 “(F) Assisting the heads of components
2 and Component Acquisition Executives in ef-
3 forts to comply with Federal law, the Federal
4 Acquisition Regulation, and Department acqui-
5 sition management directives.

6 “(G) Ensuring that grants and financial
7 assistance are provided only to individuals and
8 organizations that are not suspended or
9 debarred.

10 “(H) Distributing guidance throughout the
11 Department to ensure that contractors involved
12 in acquisitions, particularly contractors that ac-
13 cess the Department’s information systems and
14 technologies, adhere to relevant Department
15 policies related to physical and information se-
16 curity as identified by the Under Secretary for
17 Management.

18 “(I) Overseeing the Component Acquisition
19 Executive organizational structure to ensure
20 Component Acquisition Executives have suffi-
21 cient capabilities and comply with Department
22 acquisition policies.

23 “(3) DELEGATION OF CERTAIN ACQUISITION
24 DECISION AUTHORITY.—

1 “(A) LEVEL 3 ACQUISITIONS.—The Under
2 Secretary for Management may delegate acqui-
3 sition decision authority to the relevant Compo-
4 nent Acquisition Executive for an acquisition
5 program that has a life cycle cost estimate of
6 less than \$300,000,000.

7 “(B) LEVEL 2 ACQUISITIONS.—The Under
8 Secretary for Management may delegate acqui-
9 sition decision authority in writing to the rel-
10 evant Component Acquisition Executive for a
11 major acquisition program that has a life cycle
12 cost estimate of at least \$300,000 but not more
13 than \$1,000,000,000 if all of the following re-
14 quirements are met:

15 “(i) The component concerned pos-
16 sesses working policies, processes, and pro-
17 cedures that are consistent with Depart-
18 ment-level acquisition policy.

19 “(ii) The Component Acquisition Ex-
20 ecutive concerned has adequate, experi-
21 enced, and dedicated professional employ-
22 ees with program management training, as
23 applicable, commensurate with the size of
24 the acquisition programs and related ac-
25 tivities delegated to such Component Ac-

1 quisition Executive by the Under Secretary
2 for Management.

3 “(iii) Each major acquisition program
4 concerned has written documentation
5 showing that it has a Department-ap-
6 proved acquisition program baseline and it
7 is meeting agreed-upon cost, schedule, and
8 performance thresholds.

9 “(C) LEVEL 1 ACQUISITIONS.—The Under
10 Secretary for Management may delegate acqui-
11 sition decision authority in writing to the rel-
12 evant Component Acquisition Executive for a
13 Level 1 major acquisition program that has a
14 life cycle cost estimate of more than
15 \$1,000,000,000 if all of the following require-
16 ments are met:

17 “(i) The Undersecretary for Manage-
18 ment conducts a risk assessment of the
19 planned acquisition and determines that it
20 is appropriate to delegate authority for
21 such major acquisition program.

22 “(ii) The component concerned pos-
23 sesses working policies, processes, and pro-
24 cedures that are consistent with Depart-
25 ment-level acquisition policy.

1 “(iii) The Component Acquisition Ex-
2 ecutive concerned has adequate, experi-
3 enced, and dedicated professional employ-
4 ees with program management training, as
5 applicable, commensurate with the size of
6 the acquisition programs and related ac-
7 tivities delegated to such Component Ac-
8 quisition Executive by the Under Secretary
9 for Management.

10 “(iv) Each Level 1 major acquisition
11 program concerned has written documenta-
12 tion showing that it has a Department-ap-
13 proved acquisition program baseline and it
14 is meeting agreed-upon cost, schedule, and
15 performance thresholds.

16 “(v) The Under Secretary for Man-
17 agement provides written notification to
18 the appropriate congressional committees
19 of the decision to delegate the authority to
20 the relevant Component Acquisition Execu-
21 tive.

22 “(4) RELATIONSHIP TO UNDER SECRETARY
23 FOR SCIENCE AND TECHNOLOGY.—

24 “(A) IN GENERAL.—Nothing in this sub-
25 section shall diminish the authority granted to

1 the Under Secretary for Science and Tech-
2 nology under this Act. The Under Secretary for
3 Management and the Under Secretary for
4 Science and Technology shall cooperate in mat-
5 ters related to the coordination of acquisitions
6 across the Department so that investments of
7 the Directorate of Science and Technology are
8 able to support current and future requirements
9 of the components of the Department.

10 “(B) OPERATIONAL TESTING AND EVALUA-
11 TION.—The Under Secretary for Science and
12 Technology shall—

13 “(i) ensure, in coordination with rel-
14 evant component heads, that major acqui-
15 sition programs—

16 “(I) complete operational testing
17 and evaluation of technologies and
18 systems to be acquired or developed
19 by major acquisition programs to as-
20 sess operational effectiveness, suit-
21 ability, and cybersecurity;

22 “(II) use independent verification
23 and validation of operational test and
24 evaluation implementation and re-
25 sults, as appropriate; and

1 “(III) document whether such
2 programs meet all performance re-
3 quirements included in their acquisi-
4 tion program baselines;

5 “(ii) ensure that such operational
6 testing and evaluation includes all system
7 components and incorporates operators
8 into the testing to ensure that systems per-
9 form as intended in the appropriate oper-
10 ational setting; and

11 “(iii) determine if testing conducted
12 by other Federal departments and agencies
13 and private entities is relevant and suffi-
14 cient in determining whether systems per-
15 form as intended in the operational set-
16 ting.”.

17 **SEC. 123. ACQUISITION AUTHORITIES FOR UNDER SEC-**
18 **RETARY OF STRATEGY, POLICY, AND PLANS.**

19 Subsection (c) of section 709 of the Homeland Secu-
20 rity Act of 2002 (6 U.S.C. 349) is amended by—

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

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

1 “(4) ensure acquisition programs (as such term
2 is defined in section 836) support the DHS Quad-
3 rennial Homeland Security Review Report, the DHS
4 Strategic Plan, the DHS Strategic Priorities, and
5 other appropriate successor documents;”.

6 **SEC. 124. ACQUISITION AUTHORITIES FOR PROGRAM AC-**
7 **COUNTABILITY AND RISK MANAGEMENT**
8 **(PARM).**

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

13 **“SEC. 714. ACQUISITION AUTHORITIES FOR PROGRAM AC-**
14 **COUNTABILITY AND RISK MANAGEMENT.**

15 “(a) ESTABLISHMENT OF OFFICE.—Within the Man-
16 agement Directorate, there shall be a Program Account-
17 ability and Risk Management office to—

18 “(1) provide consistent accountability, stand-
19 ardization, and transparency of major acquisition
20 programs of the Department;

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

23 “(3) provide review and analysis of Department
24 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

1 the executive secretariat for the Department's Ac-
2 quisition Review Board.

3 “(5) Advise the persons having acquisition deci-
4 sion authority in making acquisition decisions con-
5 sistent with all applicable laws and in establishing
6 clear lines of authority, accountability, and responsi-
7 bility for acquisition decisionmaking within the De-
8 partment.

9 “(6) Assist the Chief Procurement Officer of
10 the Department, as appropriate, in developing strat-
11 egies and specific plans for hiring, training, and pro-
12 fessional development to address any deficiency with-
13 in the Department's acquisition workforce.

14 “(7) Develop standardized certification stand-
15 ards in consultation with the Component Acquisition
16 Executives for all acquisition program managers.

17 “(8) Assess the results of major acquisition pro-
18 grams' post-implementation reviews and identify op-
19 portunities to improve performance throughout the
20 acquisition process.

21 “(9) Provide technical support and assistance
22 to Department acquisition programs and acquisition
23 personnel and coordinate with the Chief Procure-
24 ment Officer regarding workforce training and devel-
25 opment activities.

1 “(10) Assist, as appropriate, with the prepara-
2 tion of the Future Years Homeland Security Pro-
3 gram, and make such information available to the
4 congressional homeland security committees.

5 “(c) RESPONSIBILITIES OF COMPONENTS.—Each
6 head of a component shall comply with Federal law, the
7 Federal Acquisition Regulation, and Department acquisi-
8 tion management directives established by the Under Sec-
9 retary for Management. For each major acquisition pro-
10 gram, each head of a component shall—

11 “(1) define baseline requirements and document
12 changes to such requirements, as appropriate;

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

17 “(3) verify each life cycle cost estimate against
18 independent cost estimates or assessments, as appro-
19 priate, and reconcile any differences;

20 “(4) complete a cost-benefit analysis with sup-
21 porting documentation;

22 “(5) develop and maintain a schedule that is
23 consistent with scheduling best practices as identi-
24 fied by the Comptroller General of the United

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

3 “(6) ensure that all acquisition program infor-
4 mation provided by the component is complete, accu-
5 rate, timely, and valid.

6 “(d) DEFINITIONS.—In this section:

7 “(1) ACQUISITION.—The term ‘acquisition’ has
8 the meaning given such term in section 131 of title
9 41, United States Code.

10 “(2) ACQUISITION DECISION AUTHORITY.—The
11 term ‘acquisition decision authority’ means the au-
12 thority, held by the Secretary acting through the
13 Deputy Secretary or Under Secretary for Manage-
14 ment to—

15 “(A) ensure compliance with Federal law,
16 the Federal Acquisition Regulation, and De-
17 partment acquisition management directives;

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

21 “(C) ensure that acquisition program man-
22 agers have the resources necessary to success-
23 fully execute an approved acquisition program;

24 “(D) ensure good acquisition program
25 management of cost, schedule, risk, and system

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

5 “(E) ensure that acquisition program man-
6 agers, on an ongoing basis, monitor cost, sched-
7 ule, and performance against established base-
8 lines and use tools to assess risks to an acquisi-
9 tion program at all phases of the life cycle of
10 such program to avoid and mitigate acquisition
11 program baseline breaches.

12 “(3) ACQUISITION DECISION EVENT.—The term
13 ‘acquisition decision event’, with respect to an acqui-
14 sition program, means a predetermined point within
15 each of the acquisition phases at which the acquisi-
16 tion decision authority determines whether such ac-
17 quisition program shall proceed to the next acquisi-
18 tion phase.

19 “(4) ACQUISITION PROGRAM.—The term ‘acqui-
20 sition program’ means the process by which the De-
21 partment acquires, with any appropriated amounts
22 or fee funding, by contract for purchase or lease,
23 property or services (including construction) that
24 support the missions and goals of the Department.

1 “(5) ACQUISITION PROGRAM BASELINE.—The
2 term ‘acquisition program baseline’, with respect to
3 an acquisition program, means a summary of the
4 cost, schedule, and performance parameters, ex-
5 pressed in standard, measurable, quantitative terms,
6 which must be met in order to accomplish the goals
7 of such program.

8 “(6) BEST PRACTICES.—The term ‘best prac-
9 tices’, with respect to acquisition, means a knowl-
10 edge-based approach to capability development that
11 includes the following:

12 “(A) Identifying and validating needs.

13 “(B) Assessing alternatives to select the
14 most appropriate solution.

15 “(C) Clearly establishing well-defined re-
16 quirements.

17 “(D) Developing realistic cost assessments
18 and schedules.

19 “(E) Securing stable funding that matches
20 resources to requirements.

21 “(F) Demonstrating technology, design,
22 and manufacturing maturity.

23 “(G) Using milestones and exit criteria or
24 specific accomplishments that demonstrate
25 progress.

1 “(H) Adopting and executing standardized
2 processes with known success across programs.

3 “(I) Establishing an adequate workforce
4 that is qualified and sufficient to perform nec-
5 essary functions.

6 “(J) Integrating the capabilities described
7 in subparagraphs (A) through (I) into the De-
8 partment’s mission and business operations.

9 “(7) BREACH.—The term ‘breach’, with respect
10 to a major acquisition program, means a failure to
11 meet any cost, schedule, or performance threshold
12 specified in the most recently approved acquisition
13 program baseline.

14 “(8) CONGRESSIONAL HOMELAND SECURITY
15 COMMITTEES.—The term ‘congressional homeland
16 security committees’ means—

17 “(A) the Committee on Homeland Security
18 of the House of Representatives and the Com-
19 mittee on Homeland Security and Govern-
20 mental Affairs of the Senate; and

21 “(B) the Committee on Appropriations of
22 the House of Representatives and the Com-
23 mittee on Appropriations of the Senate.

24 “(9) COMPONENT ACQUISITION EXECUTIVE.—
25 The term ‘Component Acquisition Executive’ means

1 the senior acquisition official within a component
2 who is designated in writing by the Under Secretary
3 for Management, in consultation with the component
4 head, with authority and responsibility for leading a
5 process and staff to provide acquisition and program
6 management oversight, policy, and guidance to en-
7 sure that statutory, regulatory, and higher level pol-
8 icy requirements are fulfilled, including compliance
9 with Federal law, the Federal Acquisition Regula-
10 tion, and Department acquisition management direc-
11 tives established by the Under Secretary for Man-
12 agement.

13 “(10) MAJOR ACQUISITION PROGRAM.—The
14 term ‘major acquisition program’ means a Depart-
15 ment acquisition program that is estimated by the
16 Secretary to require an eventual total expenditure of
17 at least \$300,000,000 (based on fiscal year 2019
18 constant dollars) over its life cycle cost or a program
19 identified by the Chief Acquisition Officer as a pro-
20 gram of special interest.”.

21 (b) CLERICAL AMENDMENT.—The table of contents
22 in section 1(b) of the Homeland Security Act of 2002 is
23 amended by inserting after the item relating to section
24 713, as added by this title, the following new item:

“Sec. 714. Acquisition authorities for Program Accountability and Risk Man-
agement.”.

1 **SEC. 125. GOVERNMENT ACCOUNTABILITY OFFICE REVIEW**
2 **OF BOARD AND OF REQUIREMENTS TO RE-**
3 **DUCE DUPLICATION IN ACQUISITION PRO-**
4 **GRAMS.**

5 (a) REVIEW REQUIRED.—The Comptroller General
6 of the United States shall conduct a review of the effec-
7 tiveness of the Acquisition Review Board established
8 under section 836 of the Homeland Security Act of 2002
9 (as added by this title) and the requirements to reduce
10 unnecessary duplication in acquisition programs estab-
11 lished under section 837 of such Act (as added by this
12 title) in improving the Department’s acquisition manage-
13 ment process.

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

16 (1) An assessment of the effectiveness of the
17 Board in increasing program management oversight,
18 best practices and standards, and discipline among
19 the components of the Department, including in
20 working together and in preventing overlap and un-
21 necessary duplication.

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

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

1 from moving forward in the phases of the acquisition
2 life cycle process, and the number of major acquisi-
3 tion programs that have been halted because of
4 problems with operational effectiveness, schedule
5 delays, or cost overruns.

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

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

18 **SEC. 126. EXCLUDED PARTY LIST SYSTEM WAIVERS.**

19 Not later than five days after the issuance of a waiver
20 by the Secretary of Homeland Security of Federal require-
21 ments that an agency not engage in business with a con-
22 tractor in the Excluded Party List System (or successor
23 system) as maintained by the General Services Adminis-
24 tration, the Secretary shall submit to Congress notice of
25 such waiver and an explanation for a finding by the Sec-

1 retary that a compelling reason exists for issuing such
2 waiver.

3 **SEC. 127. INSPECTOR GENERAL OVERSIGHT OF SUSPEN-**
4 **SION AND DEBARMENT.**

5 The Inspector General of the Department of Home-
6 land Security shall—

7 (1) conduct audits as determined necessary by
8 the Inspector General regarding grant and procure-
9 ment awards to identify instances in which a con-
10 tract or grant was improperly awarded to a sus-
11 pended or debarred entity and whether corrective ac-
12 tions were taken to prevent recurrence; and

13 (2) review the suspension and debarment pro-
14 gram throughout the Department to assess whether
15 suspension and debarment criteria are consistently
16 applied throughout the Department and whether dis-
17 parities exist in the application of such criteria, par-
18 ticularly with respect to business size and categories.

19 **SEC. 128. CONGRESSIONAL NOTIFICATION FOR MAJOR AC-**
20 **QUISITION PROGRAMS.**

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

1 **“SEC. 837. CONGRESSIONAL NOTIFICATION AND OTHER RE-**
2 **QUIREMENTS FOR MAJOR ACQUISITION PRO-**
3 **GRAM BREACH.**

4 “(a) REQUIREMENTS WITHIN DEPARTMENT IN
5 EVENT OF BREACH.—

6 “(1) NOTIFICATIONS.—

7 “(A) NOTIFICATION OF BREACH.—If a
8 breach occurs in a major acquisition program,
9 the program manager for such program shall
10 notify the Component Acquisition Executive for
11 such program, the head of the component con-
12 cerned, the Executive Director of the Program
13 Accountability and Risk Management division,
14 the Under Secretary for Management, and the
15 Deputy Secretary not later than 30 calendar
16 days after such breach is identified.

17 “(B) NOTIFICATION TO SECRETARY.—If a
18 breach occurs in a major acquisition program
19 and such breach results in a cost overrun great-
20 er than 15 percent, a schedule delay greater
21 than 180 days, or a failure to meet any of the
22 performance thresholds from the cost, schedule,
23 or performance parameters specified in the
24 most recently approved acquisition program
25 baseline for such program, the Component Ac-
26 quisition Executive for such program shall no-

1 tify the Secretary and the Inspector General of
2 the Department not later than five business
3 days after the Component Acquisition Executive
4 for such program, the head of the component
5 concerned, the Executive Director of the Pro-
6 gram Accountability and Risk Management Di-
7 vision, the Under Secretary for Management,
8 and the Deputy Secretary are notified of the
9 breach pursuant to subparagraph (A).

10 “(2) REMEDIATION PLAN AND ROOT CAUSE
11 ANALYSIS.—

12 “(A) IN GENERAL.—If a breach occurs in
13 a major acquisition program, the program man-
14 ager for such program shall submit to the head
15 of the component concerned, the Executive Di-
16 rector of the Program Accountability and Risk
17 Management division, and the Under Secretary
18 for Management in writing a remediation plan
19 and root cause analysis relating to such breach
20 and program. Such plan and analysis shall be
21 submitted at a date established at the discretion
22 of the Under Secretary for Management.

23 “(B) REMEDIATION PLAN.—The remedi-
24 ation plan required under this subparagraph
25 (A) shall—

1 “(i) explain the circumstances of the
2 breach at issue;

3 “(ii) provide prior cost estimating in-
4 formation;

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

12 “(I) unrealistic performance ex-
13 pectations;

14 “(II) unrealistic baseline esti-
15 mates for cost or schedule or changes
16 in program requirements;

17 “(III) immature technologies or
18 excessive manufacturing or integra-
19 tion risk;

20 “(IV) unanticipated design, engi-
21 neering, manufacturing, or technology
22 integration issues arising during pro-
23 gram performance;

24 “(V) changes to the scope of such
25 program;

1 “(VI) inadequate program fund-
2 ing or changes in planned out-year
3 funding from one 5-year funding plan
4 to the next 5-year funding plan as
5 outlined in the Future Years Home-
6 land Security Program required under
7 section 874;

8 “(VII) legislative, legal, or regu-
9 latory changes; or

10 “(VIII) inadequate program
11 management personnel, including lack
12 of sufficient number of staff, training,
13 credentials, certifications, or use of
14 best practices;

15 “(iv) propose corrective action to ad-
16 dress cost growth, schedule delays, or per-
17 formance issues;

18 “(v) explain the rationale for why a
19 proposed corrective action is recommended;
20 and

21 “(vi) in coordination with the Compo-
22 nent Acquisition Executive for such pro-
23 gram, discuss all options considered, in-
24 cluding the estimated impact on cost,
25 schedule, or performance of such program

1 if no changes are made to current require-
2 ments, the estimated cost of such program
3 if requirements are modified, and the ex-
4 tent to which funding from other programs
5 will need to be reduced to cover the cost
6 growth of such program.

7 “(3) REVIEW OF CORRECTIVE ACTIONS.—

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

15 “(B) SUBMISSION TO CONGRESS.—Not
16 later than 30 days after the review required
17 under subparagraph (A) is completed, the
18 Under Secretary for Management shall submit
19 to the congressional homeland security commit-
20 tees the following:

21 “(i) A copy of the remediation plan
22 and the root cause analysis required under
23 paragraph (2).

24 “(ii) A statement describing the cor-
25 rective action or actions that have occurred

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

4 “(b) REQUIREMENTS RELATING TO CONGRESSIONAL
5 NOTIFICATION IF BREACH OCCURS.—

6 “(1) NOTIFICATION TO CONGRESS.—If a notifi-
7 cation to the Secretary is made under subsection
8 (a)(1)(B) relating to a breach in a major acquisition
9 program, the Under Secretary for Management shall
10 notify the congressional homeland security commit-
11 tees of such breach in the next quarterly Com-
12 prehensive Acquisition Status Report, as required by
13 title I of division D of the Consolidated Appropria-
14 tions Act, 2016, (Public Law 114–113) following re-
15 ceipt by the Under Secretary of notification under
16 such subsection.

17 “(2) SIGNIFICANT VARIANCES IN COSTS OR
18 SCHEDULE.—If a likely cost overrun is greater than
19 20 percent or a likely delay is greater than 12
20 months from the costs and schedule specified in the
21 acquisition program baseline for a major acquisition
22 program, the Under Secretary for Management shall
23 include in the notification required in paragraph (1)
24 a written certification, with supporting explanation,
25 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 congressional
14 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 Security
24 rity Program.

1 “(2) FORM.—The strategy required under para-
2 graph (1) shall be submitted in unclassified form but
3 may include a classified annex for any sensitive or
4 classified information if necessary. The Secretary
5 shall publish such strategy in an unclassified format
6 that is publicly available.

7 “(b) CONSULTATION.—In developing the strategy re-
8 quired under subsection (a), the Secretary shall, as the
9 Secretary determines appropriate, consult with head-
10 quarters, components, employees in the field, and individ-
11 uals from industry and the academic community.

12 “(c) CONTENTS OF STRATEGY.—The strategy shall
13 include the following:

14 “(1) PRIORITIZED LIST.—A systematic and in-
15 tegrated prioritized list developed by the Under Sec-
16 retary for Management in coordination with all of
17 the Component Acquisition Executives of Depart-
18 ment major acquisition programs that Department
19 and component acquisition investments seek to ad-
20 dress, including the expected security and economic
21 benefit of the program or system that is the subject
22 of acquisition and an analysis of how the security
23 and economic benefit derived from such program or
24 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;

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

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

3 “(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.

4 “(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—

5 “(A) prevent cost overruns;

6 “(B) avoid schedule delays; and

7 “(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,

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

3 “(2) ADDITIONAL MATTERS COVERED.—The
4 acquisition workforce plan under this subsection
5 shall address ways to—

6 “(A) improve the recruitment, hiring,
7 training, and retention of Department acquisi-
8 tion workforce personnel, including contracting
9 officer’s representatives, in order to retain high-
10 ly qualified individuals who have experience in
11 the acquisition life cycle, complex procurements,
12 and management of large programs;

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

17 “(C) prevent duplication within Depart-
18 ment acquisition workforce training and certifi-
19 cation requirements through leveraging already-
20 existing training within the Federal Govern-
21 ment, academic community, or private industry;

22 “(D) achieve integration and consistency
23 with Government-wide training and accredita-
24 tion standards, acquisition training tools, and
25 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

1 “(iii) implementing actions to improve
2 training based on such assessments; and

3 “(G) identify ways to increase training for
4 relevant investigators and auditors of the De-
5 partment to examine fraud in major acquisition
6 programs, including identifying opportunities to
7 leverage existing Government and private sector
8 resources in coordination with the Inspector
9 General of the Department.”.

10 (b) CLERICAL AMENDMENT.—The table of contents
11 in section 1(b) of the Homeland Security Act of 2002 is
12 amended by inserting after the item relating to section
13 837, as added by this title, the following new item:

“Sec. 838. Multiyear acquisition strategy.”.

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

16 (1) REVIEW.—After submission of the first
17 multiyear acquisition strategy in accordance with
18 section 838 of the Homeland Security Act of 2002,
19 as added by subsection (a), after the date of the en-
20 actment of this Act, the Comptroller General of the
21 United States shall conduct a review of such plan
22 within 180 days to analyze the viability of such
23 plan’s effectiveness in the following:

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

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

4 (C) Demonstrating that Department acqui-
5 sition policy reflects program management best
6 practices and standards.

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

9 (E) Considering potential cost savings
10 through using already-existing technologies
11 when developing acquisition program require-
12 ments.

13 (F) Preventing duplication within Depart-
14 ment acquisition workforce training require-
15 ments through leveraging already-existing train-
16 ing within the Federal Government, academic
17 community, or private industry.

18 (G) Providing incentives for acquisition
19 program managers to reduce acquisition and
20 procurement costs through the use of best prac-
21 tices and disciplined program management.

22 (2) DEFINITIONS.—The terms “acquisition”,
23 “best practices”, and “major acquisition programs”
24 have the meanings given such terms in section 836

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

3 (3) REPORT.—Not later than 180 days after
4 the completion of the review required by subsection
5 (a), the Comptroller General of the United States
6 shall submit to the Committee on Homeland Secu-
7 rity and the Committee on Appropriations of the
8 House of Representatives and the Committee on
9 Homeland Security and Governmental Affairs and
10 the Committee on Appropriations of the Senate a re-
11 port on the review. Such report shall be submitted
12 in unclassified form but may include a classified
13 annex.

14 **SEC. 130. ACQUISITION REPORTS.**

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

19 **“SEC. 839. ACQUISITION REPORTS.**

20 “(a) COMPREHENSIVE ACQUISITION STATUS RE-
21 PORT.—

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

1 submit to the congressional homeland security com-
2 mittees an annual comprehensive acquisition status
3 report. The report shall include the following:

4 “(A) The information required under the
5 heading ‘Office of the Under Secretary for
6 Management’ under title I of division D of the
7 Consolidated Appropriations Act, 2012 (Public
8 Law 112–74) (as required under the Depart-
9 ment of Homeland Security Appropriations Act,
10 2013 (Public Law 113–6)).

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

17 “(C) A listing of established Executive
18 Steering Committees, which provide governance
19 of a program or related set of programs and
20 lower-tiered oversight, and support between ac-
21 quisition decision events and component re-
22 views, including the mission and membership
23 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.

1 “(F) A rating of cost risk, schedule risk,
2 and technical risk associated with the program
3 (including narrative descriptions and mitigation
4 actions).

5 “(G) Contract status (including earned
6 value management data as applicable).

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

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

12 “(b) QUARTERLY PROGRAM ACCOUNTABILITY RE-
13 PORT.—The Under Secretary for Management shall pre-
14 pare a quarterly program accountability report to meet the
15 mandate of the Department to perform program health
16 assessments and improve program execution and govern-
17 ance. The report shall be submitted to the congressional
18 homeland security committees.

19 “(c) CONGRESSIONAL HOMELAND SECURITY COM-
20 MITTEES DEFINED.—In this section, the term ‘congres-
21 sional homeland security committees’ means—

22 “(1) the Committee on Homeland Security of
23 the House of Representatives and the Committee on
24 Homeland Security and Governmental Affairs of the
25 Senate; and

1 “(2) the Committee on Appropriations of the
2 House of Representatives and the Committee on Ap-
3 propriations of the Senate.”.

4 (b) LEVEL 3 ACQUISITION PROGRAMS OF COMPO-
5 NENTS OF THE DEPARTMENT.—

6 (1) IN GENERAL.—Not later than 60 days after
7 the date of the enactment of this Act, component
8 heads of the Department of Homeland Security shall
9 identify to the Under Secretary for Management of
10 the Department all level 3 acquisition programs of
11 each respective component. Not later than 30 days
12 after receipt of such information, the Under Sec-
13 retary shall certify in writing to the congressional
14 homeland security committees whether such compo-
15 nent heads have properly identified such programs.
16 To carry out this paragraph, the Under Secretary
17 shall establish a process with a repeatable method-
18 ology to continually identify level 3 acquisition pro-
19 grams.

20 (2) POLICIES AND GUIDANCE.—Not later than
21 180 days after the date of the enactment of this Act,
22 component heads of the Department of Homeland
23 Security shall submit to the Under Secretary for
24 Management of the Department their respective
25 policies and relevant guidance for level 3 acquisition

1 programs of each respective component. Not later
2 than 90 days after receipt of such policies and guid-
3 ance, the Under Secretary for Management shall
4 certify to the congressional homeland security com-
5 mittees that each component's respective policies
6 and guidance adhere to Department-wide acquisition
7 policies.

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

“Sec. 839. Acquisition reports.”.

12 **SEC. 131. PROHIBITION ON OPERATION OR PROCUREMENT**
13 **OF FOREIGN-MADE UNMANNED AIRCRAFT**
14 **SYSTEMS.**

15 (a) PROHIBITION ON AGENCY OPERATION OR PRO-
16 CUREMENT.—The Secretary of Homeland Security may
17 not operate, provide financial assistance for, or enter into
18 or renew a contract for the procurement of—

- 19 (1) an unmanned aircraft system (UAS) that—
20 (A) is manufactured in a covered foreign
21 country or by a corporation domiciled in a cov-
22 ered foreign country;
23 (B) uses flight controllers, radios, data
24 transmission devices, cameras, or gimbals man-
25 ufactured in a covered foreign country or by a

1 corporation domiciled in a covered foreign coun-
2 try;

3 (C) uses a ground control system or oper-
4 ating software developed in a covered foreign
5 country or by a corporation domiciled in a cov-
6 ered foreign country; or

7 (D) uses network connectivity or data stor-
8 age located in or administered by a corporation
9 domiciled in a covered foreign country; or

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

14 (b) WAIVER.—The Secretary of Homeland Security
15 may waive the prohibition under subsection (a) on a case
16 by case basis by certifying in writing to the Committee
17 on Homeland Security of the House of Representatives
18 and the Committee on Homeland Security and Govern-
19 mental Affairs of the Senate that the operation or procure-
20 ment that is the subject of such a waiver is required—

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

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

1 (3) for intelligence, electronic warfare, or infor-
2 mation warfare operations, testing, analysis, and or
3 training.

4 (c) DEFINITIONS.—In this section:

5 (1) COVERED FOREIGN COUNTRY.—The term
6 “covered foreign country” means a country labeled
7 as a strategic competitor in the “Summary of the
8 2018 National Defense Strategy of the United
9 States of America: Sharpening the American Mili-
10 tary’s Competitive Edge” issued by the Department
11 of Defense pursuant to section 113 of title 10,
12 United States Code.

13 (2) COVERED UNMANNED AIRCRAFT SYSTEM.—
14 The term “unmanned aircraft system” has the
15 meaning given such term in section 331 of the FAA
16 Modernization and Reform Act of 2012 (Public Law
17 112–95; 49 U.S.C. 44802 note).

18 **SEC. 132. ESTABLISHMENT OF THE OFFICE OF BIOMETRIC**
19 **IDENTITY MANAGEMENT.**

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

1 **“SEC. 715. OFFICE OF BIOMETRIC IDENTITY MANAGEMENT.**

2 “(a) ESTABLISHMENT.—The Office of Biometric
3 Identity Management is established within the Manage-
4 ment Directorate of the Department.

5 “(b) DIRECTOR.—

6 “(1) IN GENERAL.—The Office of Biometric
7 Identity Management shall be administered by the
8 Director of the Office of Biometric Identity Manage-
9 ment (in this section referred to as the ‘Director’)
10 who shall report to the Secretary, or to another offi-
11 cial of the Department, as the Secretary may direct.

12 “(2) QUALIFICATIONS AND DUTIES.—The Di-
13 rector shall—

14 “(A) have significant professional manage-
15 ment experience, as well as experience in the
16 field of biometrics and identity management;

17 “(B) lead the Department’s biometric iden-
18 tity services to support efforts and activities re-
19 lating to anti-terrorism, counter-terrorism, bor-
20 der security, credentialing, national security,
21 and public safety;

22 “(C) enable operational missions across the
23 Department by receiving, matching, storing,
24 sharing, and analyzing biometric and associated
25 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-

1 formity, and work to make such standards Gov-
2 ernment-wide;

3 “(I) in coordination with the Department’s
4 Office of Strategy, Policy, and Plans, and in
5 consultation with relevant component offices
6 and headquarters offices, enter into data shar-
7 ing agreements with appropriate Federal, State,
8 local, and foreign agencies to support immigra-
9 tion, law enforcement, national security, and
10 public safety missions;

11 “(J) maximize interoperability with other
12 Federal, State, local, and foreign biometric sys-
13 tems, as appropriate;

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

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

21 “(c) DEPUTY DIRECTOR.—There shall be in the Of-
22 fice of Biometric Identity Management a Deputy Director,
23 who shall assist the Director in the management of the
24 Office.

25 “(d) OTHER AUTHORITIES.—

1 “(1) IN GENERAL.—The Director may establish
2 such other offices within the Office of Biometric
3 Identity Management as the Director determines
4 necessary to carry out the missions, duties, func-
5 tions, and authorities of the Office.

6 “(2) NOTIFICATION.—If the Director exercises
7 the authority provided by paragraph (1), the Direc-
8 tor shall notify the Committee on Homeland Secu-
9 rity of the House of Representatives and the Com-
10 mittee on Homeland Security and Governmental Af-
11 fairs of the Senate not later than 30 days before ex-
12 ercising such authority.”.

13 (b) CLERICAL AMENDMENT.—The table of contents
14 in section 1(b) of the Homeland Security Act of 2002 is
15 amended by inserting after the item relating to section
16 714, as added by this title, the following new item:

“Sec. 715. Office of Biometric Identity Management.”.

17 **Subtitle C—Management of**
18 **Programs**

19 **SEC. 141. DEPARTMENT OF HOMELAND SECURITY EN-**
20 **HANCED HIRING.**

21 (a) APPOINTMENT AUTHORITY FOR VETERANS.—
22 Notwithstanding sections 3309 through 3319, 3327, and
23 3330 of title 5, United States Code, the Secretary of
24 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

1 number of qualified candidates appointed under
2 this section does not exceed 20 percent of the
3 total number of positions that the Department
4 of Homeland Security filled during the pre-
5 ceding fiscal year.

6 (c) REGULATIONS.—The Secretary of Homeland Se-
7 curity may prescribe regulations to carry out this section
8 and any such regulations shall be exempt from the require-
9 ments of section 553 of title 5, United States Code, as
10 a matter relating to agency management or personnel.

11 (d) INFORMATION AND REPORT.—

12 (1) INFORMATION.—The Secretary of Home-
13 land Security shall, not later than December 31 of
14 each calendar year, provide to the Director of the
15 Office of Personnel Management identification of the
16 mission critical occupations to which the Secretary
17 appointed qualified candidates under subsection (b)
18 during the preceding fiscal year.

19 (2) REPORT.—The Secretary of Homeland Se-
20 curity shall annually report to Congress on the effec-
21 tiveness of the use of the authority under this sec-
22 tion regarding the length of time to hire individuals,
23 employee retention, and vacancies within the Depart-
24 ment of Homeland Security.

25 (e) DEFINITIONS.—In this section—

1 (1) the term “veteran” means an individual
2 who—

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

5 (ii) was discharged or released from active
6 duty in the Armed Forces under honorable con-
7 ditions; or

8 (B) is preference eligible, as defined in sec-
9 tion 2108 of title 5, United States Code; and

10 (2) the term “mission critical occupation”
11 means those occupations that affect the ability to
12 achieve the agency’s mission.

13 **SEC. 142. FITNESS STANDARDS.**

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

20 (1) develop a strategy and timeline for imple-
21 mentation and use of uniform fitness standards that
22 correspond to the relevant position risk level as the
23 basis for fitness determinations for a contractor em-
24 ployee across the Department of Homeland Security;
25 and

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

3 (b) LENGTH OF TIME FOR FITNESS REVIEW.—The
4 Secretary of Homeland Security, acting through the Chief
5 Security Officer of the Department of Homeland Security,
6 shall collect data to allow the Department and its compo-
7 nents and contractor representatives to assess average fit-
8 ness investigation, adjudication, and determination proc-
9 essing times for each component of the Department, in-
10 cluding information regarding the parameters used to cal-
11 culate each such average.

12 (c) STUDY ON FITNESS ADJUDICATION STATUS UP-
13 DATES.—Not later than one year after the date of the en-
14 actment of this Act, the Secretary of Homeland Security,
15 acting through the Chief Security Officer of the Depart-
16 ment of Homeland Security, shall enter into a contract
17 with a federally funded research and development center
18 (FFRDC) to conduct a cost benefit analysis for estab-
19 lishing a uniform process to provide contractor representa-
20 tives access to information regarding the status of fitness
21 determinations for Department contractor employees rel-
22 evant to such contractor representatives.

1 **SEC. 143. TRAINING TO PROTECT THE VULNERABLE.**

2 (a) TRAINING EXPANSION.—Section 884(c) of the
3 Homeland Security Act of 2002 (6 U.S.C. 464) is amend-
4 ed—

5 (1) in paragraph (9), by striking “and” at the
6 end;

7 (2) by redesignating paragraph (10) as para-
8 graph (11); and

9 (3) by inserting after paragraph (9) and insert-
10 ing the following new paragraphs:

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

17 (b) FLETC HUMAN TRAFFICKING AWARENESS
18 TRAINING PROGRAM.—The Director, in consultation with
19 the Blue Campaign office, shall develop a program to pro-
20 vide training to Federal, State, local, Tribal, territorial,
21 and international law enforcement personnel, as appro-
22 priate, related to—

23 (1) identifying instances of human trafficking;

24 (2) the types of information that should be col-
25 lected and recorded in information technology sys-
26 tems utilized by the Department to help identify in-

1 individuals 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.

1 **SEC. 144. DEPARTMENT OF HOMELAND SECURITY BLUE**
2 **CAMPAIGN ENHANCEMENT.**

3 Section 434 of the Homeland Security Act of 2002
4 (6 U.S.C. 242) is amended by adding at the end the fol-
5 lowing new subsections:

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

12 “(1) Federal, State, local, Tribal, and territorial
13 law enforcement officers.

14 “(2) Detention and correction system personnel.

15 “(3) Such other individuals as the Director de-
16 termines appropriate.

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

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

22 “(A) The Transportation Security Admin-
23 istration.

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

25 “(C) U.S. Immigration and Customs En-
26 forcement.

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-

1 plementation of such programs, the Director is authorized
2 to consult with State, local, Tribal, and territorial agen-
3 cies, non-governmental organizations, private sector orga-
4 nizations, and experts. Such consultation shall be exempt
5 from the Federal Advisory Committee Act (5 U.S.C.
6 App.).”.

7 **TITLE II—INTELLIGENCE AND** 8 **INFORMATION SHARING**

9 **Subtitle A—DHS Intelligence** 10 **Enterprise**

11 **SEC. 201. ANNUAL HOMELAND THREAT ASSESSMENTS.**

12 (a) IN GENERAL.—Subtitle A of title II of the Home-
13 land Security Act of 2002 (6 U.S.C. 121 et seq.) is amend-
14 ed by adding at the end the following new section:

15 **“SEC. 210H. HOMELAND THREAT ASSESSMENTS.**

16 “(a) IN GENERAL.—Not later than 180 days after
17 the date of the enactment of this section and for each of
18 the next five fiscal years (beginning in the fiscal year that
19 begins after the date of the enactment of this section) the
20 Secretary, acting through the Under Secretary for Intel-
21 ligence and Analysis, and using departmental information,
22 including component information, and information pro-
23 vided through State and major urban area fusion centers,
24 shall conduct an assessment of the terrorist threat to the
25 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

1 “(2) may include unclassified annexes, if appro-
2 priate.”.

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

7 “(24) To carry out section 210H (relating to
8 homeland threat assessments).”.

9 (c) CLERICAL AMENDMENT.—The table of contents
10 of the Homeland Security Act of 2002 is amended by in-
11 serting after the item relating to section 210G the fol-
12 lowing new item:

 “Sec. 210H. Homeland threat assessments.”.

13 **SEC. 202. HOMELAND INTELLIGENCE DOCTRINE.**

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

18 **“SEC. 210I. HOMELAND INTELLIGENCE DOCTRINE.**

19 “(a) IN GENERAL.—Not later than 180 days after
20 the date of the enactment of this section, the Secretary,
21 acting through the Chief Intelligence Officer of the De-
22 partment, in coordination with intelligence components of
23 the Department, the Office of the General Counsel, the
24 Privacy Office, and the Office for Civil Rights and Civil
25 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

1 and between Federal departments and agencies,
2 among and between State, local, Tribal, and terri-
3 torial governments, including law enforcement, and
4 with foreign partners and the private sector, con-
5 sistent with the protection of privacy, civil rights,
6 and civil liberties.

7 “(6) A description of how the dissemination to
8 the intelligence community (as such term is defined
9 in section 3(4) of the National Security Act of 1947
10 (50 U.S.C. 3003(4))) and Federal law enforcement
11 of such information assists such entities in carrying
12 out their respective missions.

13 “(c) FORM.—The guidance required under subsection
14 (a) shall be submitted in unclassified form, but may in-
15 clude a classified annex.

16 “(d) ANNUAL REVIEW.—For each of the 5 fiscal
17 years beginning with the first fiscal year that begins after
18 the date of the enactment of this section, the Secretary
19 shall conduct a review of the guidance required under sub-
20 section (a) and, as appropriate, revise such guidance.”.

21 (b) CLERICAL AMENDMENT.—The table of contents
22 in section 1(b) of the Homeland Security Act of 2002 is
23 amended by inserting after the item relating to section
24 210H, as added by title, the following new item:

“Sec. 210I. Homeland intelligence doctrine.”.

1 **SEC. 203. COMPTROLLER GENERAL ASSESSMENT.**

2 (a) ANNUAL ASSESSMENT REQUIRED.—Not later
3 than 1 year after the date of the enactment of this Act
4 and again not later than 5 years thereafter, the Comp-
5 troller General of the United States shall submit to the
6 Committee on Homeland Security of the House of Rep-
7 resentatives and the Committee on Homeland Security
8 and Governmental Affairs of the Senate an assessment of
9 the degree to which guidance established pursuant to sec-
10 tion 210I of the Homeland Security Act of 2002 (as added
11 by section 202) is implemented across the Department of
12 Homeland Security. Such assessment should evaluate the
13 extent to which such guidance is carried out in a manner
14 that protects privacy, civil rights, and civil liberties.

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

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

21 (2) include any other subject matter the Comp-
22 troller General determines appropriate.

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

1 **SEC. 204. ANALYSTS FOR THE CHIEF INTELLIGENCE OFFI-**
2 **CER.**

3 Paragraph (1) of section 201(e) of the Homeland Se-
4 curity Act of 2002 (6 U.S.C. 121(e)) is amended by add-
5 ing at the end the following new sentence: “The Secretary
6 shall also provide the Chief Intelligence Officer with a
7 staff having appropriate expertise and experience to assist
8 the Chief Intelligence Officer.”.

9 **SEC. 205. ESTABLISHMENT OF INSIDER THREAT PROGRAM.**

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

13 **“SEC. 104. INSIDER THREAT PROGRAM.**

14 “(a) ESTABLISHMENT.—The Secretary shall estab-
15 lish an Insider Threat Program within the Department.
16 Such Program shall—

17 “(1) provide training and education for Depart-
18 ment personnel to identify, prevent, mitigate, and re-
19 spond to insider threat risks to the Department’s
20 critical assets;

21 “(2) provide investigative support regarding po-
22 tential insider threats that may pose a risk to the
23 Department’s critical assets; and

24 “(3) conduct risk mitigation activities for in-
25 sider threats.

26 “(b) STEERING COMMITTEE.—

1 “(1) IN GENERAL.—The Secretary shall estab-
2 lish a Steering Committee within the Department.
3 The Under Secretary for Intelligence and Analysis
4 shall serve as the Chair of the Steering Committee.
5 The Chief Security Officer shall serve as the Vice
6 Chair. The Steering Committee shall be comprised
7 of representatives of the Office of Intelligence and
8 Analysis, the Office of the Chief Information Officer,
9 the Office of the General Counsel, the Office for
10 Civil Rights and Civil Liberties, the Privacy Office,
11 the Office of the Chief Human Capital Officer, the
12 Office of the Chief Financial Officer, the Federal
13 Protective Service, the Office of the Chief Procure-
14 ment Officer, the Science and Technology Direc-
15 torate, and other components or offices of the De-
16 partment as appropriate. Such representatives shall
17 meet on a regular basis to discuss cases and issues
18 related to insider threats to the Department’s crit-
19 ical assets, in accordance with subsection (a).

20 “(2) RESPONSIBILITIES.—Not later than one
21 year after the date of the enactment of this section,
22 the Under Secretary for Intelligence and Analysis
23 and the Chief Security Officer, in coordination with
24 the Steering Committee established pursuant to
25 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-

1 sonal services contractors, or any other category
2 of person who acts for or on behalf of the De-
3 partment, as determined by the Secretary; or

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

7 “(3) INSIDER THREAT.—The term ‘insider
8 threat’ means the threat that an insider will use his
9 or her authorized access, wittingly or unwittingly, to
10 do harm to the security of the United States, includ-
11 ing damage to the United States through espionage,
12 terrorism, the unauthorized disclosure of classified
13 national security information, or through the loss or
14 degradation of departmental resources or capabili-
15 ties.”.

16 (b) REPORTING.—

17 (1) IN GENERAL.—Not later than two years
18 after the date of the enactment of section 104 of the
19 Homeland Security Act of 2002 (as added by sub-
20 section (a) of this section) and biennially thereafter
21 for the next four years, the Secretary of Homeland
22 Security shall submit to the Committee on Home-
23 land Security and the Permanent Select Committee
24 on Intelligence of the House of Representatives and
25 the Committee on Homeland Security and Govern-

1 mental Affairs and the Select Committee on Intel-
2 ligence of the Senate a report on how the Depart-
3 ment of Homeland Security and its components and
4 offices have implemented the strategy developed pur-
5 suant to subsection (b)(2)(A) of such section 104,
6 the status of the Department's risk assessment of
7 critical assets, the types of insider threat training
8 conducted, the number of Department employees
9 who have received such training, and information on
10 the effectiveness of the Insider Threat Program (es-
11 tablished pursuant to subsection (a) of such section
12 104), based on metrics developed, collected, and re-
13 ported pursuant to subsection (b)(2)(H) of such sec-
14 tion 104.

15 (2) DEFINITIONS.—In this subsection, the
16 terms “critical assets”, “insider”, and “insider
17 threat” have the meanings given such terms in sec-
18 tion 104 of the Homeland Security Act of 2002 (as
19 added by subsection (a) of this section).

20 (c) CLERICAL AMENDMENT.—The table of contents
21 in section 1(b) of the Homeland Security Act of 2002 is
22 amended by inserting after the item relating to section
23 103 the following new item:

“Sec. 104. Insider Threat Program.”.

1 **SEC. 206. DEPARTMENT OF HOMELAND SECURITY COUN-**
2 **TERINTELLIGENCE VETTING TASK FORCE.**

3 (a) ESTABLISHMENT.—Not later than 180 days after
4 the date of the enactment of this Act, the Secretary of
5 Homeland Security shall assign personnel of the Depart-
6 ment of Homeland Security to participate in a counter-
7 intelligence vetting task force to make recommendations
8 to improve counterintelligence vetting for appropriate de-
9 partmental programs.

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

15 (c) COORDINATION.—In carrying out subsection (a),
16 the Secretary of Homeland Security may request partici-
17 pation in the task force established pursuant to such sub-
18 section from other appropriate Federal agencies.

19 (d) REPORT.—Not later than one year after the date
20 of the enactment of this Act, the Secretary of Homeland
21 Security shall submit to the Committee on Homeland Se-
22 curity of the House of Representatives and the Committee
23 on Homeland Security and Governmental Affairs of the
24 Senate a report on the recommendations made by the task
25 force established pursuant to subsection (a).

1 **SEC. 207. VISA SECURITY.**

2 (a) ESTABLISHMENT.—

3 (1) IN GENERAL.—Not later than 90 days after
4 the date of the enactment of this Act, the inter-
5 agency working group established under section
6 1746(a) of the National Defense Authorization Act
7 for Fiscal Year 2020 (Public Law 116–92) shall
8 commence a review of the current policies and proce-
9 dures of the Department of Homeland Security and
10 Department of State for the purpose of identifying,
11 investigating, and preventing the illicit transfer of
12 sensitive technologies and research from United
13 States institutions of higher education and research
14 institutions through more effective visa security op-
15 erations and improved protections for such sensitive
16 technologies.

17 (2) OBJECTIVES.—

18 (A) ANALYSIS OF CURRENT VISA ISSUANCE
19 AND ADMISSION PROCEDURES.—The inter-
20 agency working group referred to in paragraph

21 (1) shall—

22 (i) analyze the current visa applica-
23 tion process, and the role of the Depart-
24 ment of Homeland Security and the De-
25 partment of State in such process, includ-
26 ing the screening of visa applicants against

1 appropriate criminal, intelligence, national
2 security, terrorism, and other databases
3 and information maintained by the Federal
4 Government, and make recommendations
5 to the Secretaries of such Departments to
6 better screen, identify, and refuse entry to
7 individuals who seek to enter the United
8 States to engage in the illicit transfer of
9 sensitive technologies from United States
10 institutions of higher educations or re-
11 search institutions;

12 (ii) evaluate current policies for refus-
13 ing visas on grounds that an individual is
14 likely to enter the United States to engage
15 in the illicit transfer of sensitive tech-
16 nologies and recommend updates to the
17 Foreign Affairs Manual and other agency
18 guidance to clarify when and how visas can
19 be refused on such grounds; and

20 (iii) analyze current screening proce-
21 dures at United States ports of entry and
22 make recommendations to the Secretaries
23 of such Departments to better identify in-
24 dividuals who seek to enter the United

1 States to engage in such illicit transfer of
2 sensitive technologies.

3 (B) NATIONAL SECURITY REVIEW OF CER-
4 TAIN NONIMMIGRANT STUDENTS.—The inter-
5 agency working group shall recommend proce-
6 dures and standards for the Department of
7 Homeland Security, in cooperation with other
8 appropriate Federal agencies, to conduct na-
9 tional security reviews of aliens who—

10 (i) are present in the United States—

11 (I) in a nonimmigrant classifica-
12 tion described in subparagraphs (F),
13 (J), or (M) of section 101(a)(15) of
14 the Immigration and Nationality Act
15 (8 U.S.C. 1101(a)(15)) and change
16 from a program of study not related
17 to sensitive technologies to a program
18 of study or significant coursework, re-
19 search, or laboratory access related to
20 sensitive technologies; or

21 (II) as a nonimmigrant and seek
22 to change status, pursuant to section
23 248 of the Immigration and Nation-
24 ality Act (8 U.S.C. 1258)), to that of
25 a nonimmigrant described in subpara-

1 graph (F), (J), or (M) of section
2 101(a)(15) of such Act (8 U.S.C.
3 1101(a)(15)), for purposes of engag-
4 ing in a program of study related to
5 sensitive technologies; and

6 (ii) as a result of engaging in a pro-
7 gram of study related to sensitive tech-
8 nologies, will have access to information re-
9 lated to operating, installing, maintaining,
10 repairing, overhauling, or refurbishing sen-
11 sitive technologies or development activities
12 related to sensitive technologies.

13 (C) IDENTIFYING INDIVIDUALS REQUIRING
14 NATIONAL SECURITY REVIEW.—For purposes of
15 facilitating the identification of individuals de-
16 scribed in subparagraph (B)(ii), the interagency
17 working group shall—

18 (i) develop a nonpublic list of six-digit
19 Classification of Instructional Programs
20 (CIP) codes for programs of study related
21 to sensitive technologies to be used in re-
22 porting required by section 641 of the Im-
23 migration and Nationality Act (8 U.S.C.
24 1372(d)) and related regulations;

1 (ii) recommend to the Secretary of
2 Homeland Security changes, as appro-
3 priate, to the Student and Exchange Vis-
4 itor Information System, or other system
5 designated for such purpose by the Sec-
6 retary of Homeland Security, to ensure
7 that individuals who seek to engage in pro-
8 grams of study but who will not have ac-
9 cess to information related to operating,
10 installing, maintaining, repairing, over-
11 hauling, or refurbishing sensitive tech-
12 nologies or development activities related
13 to sensitive technologies are not unneces-
14 sarily subjected to national security re-
15 views;

16 (iii) recommend to the Secretary of
17 Homeland Security changes to relevant
18 regulations to ensure that entities certified
19 by the Student and Exchange Visitor Pro-
20 gram routinely and accurately report the
21 program of study and other necessary in-
22 formation in the Student and Exchange
23 Visitor Information System, or other sys-
24 tem designated for such purpose by the
25 Secretary of Homeland Security, for each

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

6 (iv) identify mechanisms for the De-
7 partment of Homeland Security, in co-
8 operation with other appropriate Federal
9 agencies, to order the removal of and make
10 ineligible for future nonimmigrant classi-
11 fication described in subparagraphs (F),
12 (J), or (M) of section 101(a)(15) of the
13 Immigration and Nationality Act (8 U.S.C.
14 1101(a)(15)) individuals who may be iden-
15 tified following pursuant to national secu-
16 rity reviews conducted in accordance with
17 subparagraph (B).

18 (D) IDENTIFYING GAPS IN AUTHORITY TO
19 ADDRESS NATIONAL SECURITY THREATS.—Not
20 later than one year after the date of the enact-
21 ment of this Act, the interagency working group
22 shall identify deficiencies in existing legal au-
23 thorities determined to be an impediment in
24 achieving the recommendations described in
25 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.

1 (H) Private sector and higher education
2 personnel, as appropriate and to a degree that
3 would not detrimentally impact any ongoing law
4 enforcement investigation or intelligence oper-
5 ation, as determined by the Secretary of Home-
6 land Security.

7 (4) CONSULTATION.—In carrying out the objec-
8 tives described in paragraph (2), the interagency
9 working group shall coordinate and consult regularly
10 with the National Science, Technology, and Security
11 Roundtable established under section 1746(b) of the
12 National Defense Authorization Act for Fiscal Year
13 2020 (Public Law 116–92).

14 (5) REPORT.—Not later than one year after the
15 commencement of the review required under para-
16 graph (1), the interagency working group shall sub-
17 mit to the appropriate congressional committees a
18 report—

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

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

1 vent the illicit transfer of sensitive technologies
2 from United States institutions of higher edu-
3 cation and research institutions as a result of
4 programs of study related to sensitive tech-
5 nologies undertaken by aliens described in sub-
6 paragraph (F), (J), or (M) of section
7 101(a)(15) of the Immigration and Nationality
8 Act (8 U.S.C. 1101(a)(15)).

9 (6) DEFINITIONS.—In this subsection:

10 (A) APPROPRIATE CONGRESSIONAL COM-
11 MITTEES.—The term “appropriate congres-
12 sional committees” means the Committee on
13 Homeland Security, the Committee on the Judi-
14 ciary, the Committee on Armed Services, and
15 the Committee on Foreign Affairs of the House
16 of Representatives and the Committee on
17 Homeland Security and Governmental Affairs,
18 the Committee on the Judiciary, the Committee
19 on Armed Services, and the Committee on For-
20 eign Relations of the Senate.

21 (B) INSTITUTION OF HIGHER EDU-
22 CATION.—The term “institution of higher edu-
23 cation” has the meaning given such term in
24 section 101 of the Higher Education Act of
25 1965 (20 U.S.C. 1001).

1 (C) PROGRAM OF STUDY.—The term “pro-
2 gram of study” means any degree program,
3 field of study, significant coursework, research,
4 or laboratory access related to sensitive tech-
5 nologies, or other academic activity required to
6 be reported pursuant to section 641(a) of the
7 Omnibus Consolidated Appropriations Act,
8 1997 (Public Law 104–208 (8 U.S.C.
9 1372(a))).

10 (D) SENSITIVE TECHNOLOGIES.—The
11 term “sensitive technologies” has the meaning
12 given such term in paragraph (8) of section
13 428(e) of the Homeland Security Act of 2002
14 (6 U.S.C. 236(e)), as added by subsection (b).

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

17 (1) PROGRAM SCOPE.—Paragraph (1) of section
18 428(e) of the Homeland Security Act of 2002 (6
19 U.S.C. 236(e)) is amended—

20 (A) by striking “The Secretary” and in-
21 serting the following:

22 “(A) AUTHORIZATION.—The Secretary”;
23 and

24 (B) by adding at the end the following new
25 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-

1 rorist organizations (as such term is
2 defined in section 212(a)(3)(B)(vi) of
3 the Immigration and Nationality Act
4 (8 U.S.C. 1182(a)(3)(B)(vi))) within
5 or through such country.

6 “(IV) The number of formal ob-
7 jections and denials based on deroga-
8 tory information issued through the
9 interagency Security Advisory Opinion
10 process.

11 “(V) Countries identified as a
12 strategic competitor in the ‘Summary
13 of the 2018 National Defense Strat-
14 egy of the United States of America:
15 Sharpening the American Military’s
16 Competitive Edge’ issued by the De-
17 partment of Defense pursuant to sec-
18 tion 113(g)(1)(A) of title 10, United
19 States Code, or any successor docu-
20 ment.

21 “(VI) The number of cases in-
22 volving counterintelligence, illicit tech-
23 nology transfer, and counterprolifera-
24 tion related to the identities of nation-
25 als of such country.

1 “(VII) Information on the co-
2 operation of such country with the
3 counterintelligence, countering non-
4 traditional collection, illicit technology
5 transfer, and counterproliferation ef-
6 forts of the United States, including
7 information on foreign government-
8 owned infrastructure and organiza-
9 tions dedicated to such matters.

10 “(VIII) The adequacy of the bor-
11 der and immigration control of such
12 country.

13 “(IX) Any other criteria the Sec-
14 retary determines appropriate.

15 “(iii) PRIORITIZATION.—The Sec-
16 retary shall, until December 31, 2024,
17 prioritize the establishment of new over-
18 seas assignments made under this sub-
19 section to diplomatic and consular posts in
20 countries that are strategic competitors
21 with the goal of countering the exploitation
22 or illicit transfer of sensitive technologies
23 by aliens described in subparagraph (F),
24 (J), or (M) of section 101(a)(15) of such
25 Act (8 U.S.C. 1101(a)(15)).”.

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

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

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

8 “(C) Review visa applications of aliens
9 against appropriate criminal, national security,
10 and terrorism databases or other relevant infor-
11 mation maintained by the Federal Government
12 to improve the detection and examination of
13 aliens whose entry into the United States would
14 pose a substantial risk of the illicit transfer of
15 sensitive technologies.”.

16 (3) DEFINITION.—Subsection (e) of section 428
17 of the Homeland Security Act of 2002 (6 U.S.C.
18 236(e)) is amended by inserting at the end the fol-
19 lowing new paragraph:

20 “(8) DEFINITION.—In this subsection, the term
21 ‘sensitive technologies’ means—

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

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

3 “(B) emerging and foundational tech-
4 nologies identified through the interagency
5 process established under section 1758 of the
6 John S. McCain National Defense Authoriza-
7 tion Act for Fiscal Year 2019 (Public Law
8 115–232);

9 “(C) sciences, technologies, and associated
10 programs of study at an institution of higher
11 education, related to energy, nuclear science,
12 nuclear engineering, or a related field for which
13 an alien who is a citizen of Iran would be de-
14 nied a visa to participate in coursework pursu-
15 ant to section 501 of the Iran Threat Reduction
16 and Syria Human Rights Act of 2012 (22
17 U.S.C. 8771); and

18 “(D) technologies and items included on
19 the Commerce Control List, the United States
20 Munitions List, the Nuclear Regulatory Com-
21 mission Controls, or the Technology Alert
22 List.”.

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

1 security and the Secretary of State shall jointly de-
2 velop and submit to the appropriate congressional
3 committees a memorandum of understanding detail-
4 ing the responsibilities of and procedures used by
5 Department of Homeland Security personnel as-
6 signed to diplomatic and consular posts under sec-
7 tion 428 of the Homeland Security Act of 2002, as
8 amended by this subsection, including visa security
9 vetting and screening activities, the collection and
10 distribution of relevant fees, and the sharing of in-
11 formation on visa refusals based on derogatory infor-
12 mation issued through the interagency Security Ad-
13 visory Opinion process.

14 (5) MACHINE READABLE TECHNOLOGY PILOT
15 PROGRAM.—

16 (A) IN GENERAL.—Not later than one year
17 after the date of the enactment of this Act, the
18 Secretary of Homeland Security and the Sec-
19 retary of State shall jointly commence a pilot
20 program at a United States diplomatic or con-
21 sular post in a country with a high volume of
22 individuals who are known to have engaged in
23 government sponsored technology transfer cam-
24 paigns. The pilot program shall—

1 (i) be conducted for not fewer than
2 365 days; and

3 (ii) assess opportunities to enhance
4 security vetting, including the use of ma-
5 chine-readable technology and applicant
6 interviews, to better defend research or
7 sensitive technologies in the United States
8 from foreign government sponsored tech-
9 nology transfer campaigns.

10 (B) MACHINE READABLE TECHNOLOGY.—

11 The Secretary of Homeland Security and the
12 Secretary of State shall jointly, as part of the
13 pilot program under subparagraph (A)—

14 (i) deploy and test equipment and
15 technology to ensure that all documents
16 collected in connection with visa applica-
17 tions are stored in a machine-readable and
18 content-searchable format compatible and
19 shareable between the Department of
20 Homeland Security and the Department of
21 State, and as appropriate, other inter-
22 agency partners;

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

1 appropriate, and ensure appropriate per-
2 sonnel from the Department of Homeland
3 Security and the Department of State have
4 access to such documents for visa security
5 vetting purposes; and

6 (iii) evaluate the use of such tech-
7 nology and supplemental documents in im-
8 proving the efficacy and efficiency of visa
9 security vetting.

10 (C) APPLICANT INTERVIEWS.—The Sec-
11 retary of Homeland Security, in coordination
12 with the Secretary of State, shall determine
13 whether additional questions or further docu-
14 mentation requests may be appropriate during
15 visa applicant in-person interviews to improve
16 visa security vetting to address evolving threats
17 to the United States.

18 (D) REPORT.—Not later than 420 days
19 after the initiation of the pilot program under
20 subparagraph (A), the Secretary of Homeland
21 Security and the Secretary of State shall jointly
22 submit to the appropriate congressional com-
23 mittees and other appropriate Federal partners
24 a report on the following:

25 (i) The results of the pilot program.

1 (ii) Recommendations for machine-
2 readable and content searchable equipment
3 and technology and supplemental docu-
4 ments under paragraph (2).

5 (iii) Recommendations for additional
6 interview questions and further docu-
7 mentation requests under paragraph (3).

8 (iv) A determination as to whether
9 and where to expand the use of tech-
10 nologies evaluated during the pilot pro-
11 gram.

12 (6) DEFINITIONS.—In this subsection:

13 (A) APPROPRIATE CONGRESSIONAL COM-
14 MITTEES.—The term “appropriate congres-
15 sional committees” means—

16 (i) the Committee on Homeland Secu-
17 rity and the Committee on Foreign Affairs
18 of the House of Representatives; and

19 (ii) the Committee on Homeland Se-
20 curity and Governmental Affairs and the
21 Committee on Foreign Relations of the
22 Senate.

23 (B) SCREENING.—The term “screening”
24 means the review of public, private, or govern-
25 mental 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-

1 mation, and information drawn from other
2 sources to reach a determination regarding a
3 national security concern related to the visa ap-
4 plicant.

5 **SEC. 208. CHEMICAL, BIOLOGICAL, RADIOLOGICAL, AND**
6 **NUCLEAR INTELLIGENCE AND INFORMATION**
7 **SHARING.**

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

12 **“SEC. 210J. CHEMICAL, BIOLOGICAL, RADIOLOGICAL, AND**
13 **NUCLEAR INTELLIGENCE AND INFORMATION**
14 **SHARING.**

15 “(a) IN GENERAL.—The Office of Intelligence and
16 Analysis, in consultation with the Director of the Coun-
17 tering Weapons of Mass Destruction Office, of the Depart-
18 ment of Homeland Security shall—

19 “(1) support homeland security-focused intel-
20 ligence analysis of terrorist actors, their claims, and
21 their plans to conduct attacks involving chemical, bi-
22 ological, radiological, or nuclear materials against
23 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.”.

1 (b) CLERICAL AMENDMENT.—The table of contents
2 in section 1(b) of the Homeland Security Act of 2002 is
3 amended by inserting after the item relating to section
4 201I, as added by this title, the following new item:

“Sec. 210J. Chemical, biological, radiological, and nuclear intelligence and in-
formation sharing.”.

5 (c) REPORT.—

6 (1) IN GENERAL.—Not later than one year
7 after the date of the enactment of this Act and an-
8 nually thereafter for each of the following four years,
9 the Secretary of Homeland Security shall report to
10 the appropriate congressional committees on the fol-
11 lowing:

12 (A) The intelligence and information shar-
13 ing activities under section 210J of the Home-
14 land Security Act of 2002 (as added by sub-
15 section (a) of this section) and of all relevant
16 entities within the Department of Homeland
17 Security to counter the threat from attacks
18 using chemical, biological, radiological, or nu-
19 clear materials.

20 (B) The Department’s activities in accord-
21 ance with relevant intelligence strategies.

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

1 (A) An assessment of the progress of the
2 Office of Intelligence and Analysis of the De-
3 partment of Homeland Security in imple-
4 menting such section 210J.

5 (B) A description of the methods estab-
6 lished to carry out such assessment.

7 (3) DEFINITION.—In this subsection, the term
8 “appropriate congressional committees” means the
9 Committee on Homeland Security of the House of
10 Representatives and the Committee on Homeland
11 Security and Governmental Affairs of the Senate
12 and any committee of the House of Representatives
13 or the Senate having legislative jurisdiction under
14 the rules of the House of Representatives or Senate,
15 respectively, over the matter concerned.

16 **SEC. 209. INLAND WATERS THREAT ANALYSIS.**

17 (a) IN GENERAL.—Not later than 180 days after the
18 date of the enactment of this Act, the Secretary of Home-
19 land Security shall submit to the appropriate congres-
20 sional committees an inland waters threat analysis that
21 includes an identification and description of the following:

22 (1) Current and potential terrorism and crimi-
23 nal threats posed by individuals and groups seeking
24 to—

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

3 (B) exploit security vulnerabilities on in-
4 land waters.

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

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

9 (B) criminal activity, as measured by the
10 total flow of illegal goods and illicit drugs, re-
11 lated to the inland waters.

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

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

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

18 (4) Vulnerabilities related to cooperation be-
19 tween State, local, Tribal, and territorial law en-
20 forcement, or international agreements, that hinder
21 effective security, counterterrorism, anti-trafficking
22 efforts, and the flow of legitimate trade with respect
23 to inland waters.

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

4 (b) ANALYSIS REQUIREMENTS.—In preparing the
5 threat analysis required under subsection (a), the Sec-
6 retary of Homeland Security shall consider and examine
7 the following:

8 (1) Technology needs and challenges.

9 (2) Personnel needs and challenges.

10 (3) The roles of State, local, Tribal, and terri-
11 torial law enforcement, as well as private sector
12 partners and the public, relating to inland waters se-
13 curity.

14 (4) The need for cooperation among Federal,
15 State, local, Tribal, territorial, and international
16 partner law enforcement, as well as private sector
17 partners and the public, relating to inland waters se-
18 curity.

19 (5) The challenges posed by geography with re-
20 spect to inland waters security.

21 (c) CLASSIFIED THREAT ANALYSIS.—To the extent
22 possible, the Secretary of Homeland Security shall submit
23 the threat analysis required under subsection (a) in un-
24 classified form. The Secretary may submit a portion of

1 the threat analysis in classified form if the Secretary de-
2 termines that such is appropriate.

3 (d) DEFINITIONS.—In this section:

4 (1) The term “appropriate congressional com-
5 mittees” means—

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

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

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

12 (2) The term “inland waters” has the meaning
13 given such term in section 83.03 of title 33, Code
14 of Federal Regulations.

15 **SEC. 210. TRANSNATIONAL CRIMINAL ORGANIZATIONS**
16 **THREAT ASSESSMENT.**

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

1 (b) RECOMMENDATIONS.—Upon completion of the
2 threat assessment required under subsection (a), the Sec-
3 retary of Homeland Security shall make a determination
4 if any changes are required to address security
5 vulnerabilities identified in such assessment.

6 (c) DISTRIBUTION.—Consistent with the protection
7 of classified and confidential unclassified information, the
8 Under Secretary for Intelligence and Analysis shall share
9 the threat assessment developed under this section with
10 State, local, and Tribal law enforcement officials, includ-
11 ing officials that operate within fusion centers in the Na-
12 tional Network of Fusion Centers.

13 **SEC. 211. DEPARTMENT OF HOMELAND SECURITY**
14 **COUNTERTERRORISM ADVISORY BOARD.**

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

19 **“SEC. 210K. DEPARTMENTAL COORDINATION ON COUNTER-**
20 **TERRORISM.**

21 “(a) ESTABLISHMENT.—There is in the Department
22 a board to be composed of senior representatives of de-
23 partmental operational components and headquarters ele-
24 ments. The purpose of the board shall be to coordinate
25 and integrate departmental intelligence, activities, and

1 policy related to the counterterrorism mission and func-
2 tions of the Department.

3 “(b) CHARTER.—There shall be a charter to govern
4 the structure and mission of the board. Such charter shall
5 direct the board to focus on the current threat environ-
6 ment and the importance of aligning departmental
7 counterterrorism activities under the Secretary’s guidance.
8 The charter shall be reviewed and updated every 4 years,
9 as appropriate.

10 “(c) MEMBERS.—

11 “(1) CHAIR.—The Secretary shall appoint a
12 Coordinator for Counterterrorism within the Depart-
13 ment who will serve as the chair of the board.

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

17 “(A) The Transportation Security Admin-
18 istration.

19 “(B) United States Customs and Border
20 Protection.

21 “(C) United States Immigration and Cus-
22 toms Enforcement.

23 “(D) The Federal Emergency Management
24 Agency.

25 “(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.

1 “(f) PROHIBITION ON ADDITIONAL FUNDS.—No ad-
2 ditional funds are authorized to carry out this section.”.

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

 “Sec. 210K. Departmental coordination on counterterrorism.”.

7 (c) REPORT.—Not later than 90 days after the date
8 of the enactment of this Act, the Secretary, acting through
9 the Coordinator for Counterterrorism, shall submit to the
10 Committee on Homeland Security of the House of Rep-
11 resentatives and the Committee on Homeland Security
12 and Governmental Affairs of the Senate a report on the
13 status and activities of the board established under section
14 210K of the Homeland Security Act of 2002, as added
15 by subsection (a).

16 **SEC. 212. NATIONAL VETTING CENTER.**

17 (a) AUTHORIZATION.—The Secretary of Homeland
18 Security, in coordination with the Secretary of State, the
19 Secretary of Defense, the Attorney General, and the Di-
20 rector of National Intelligence, shall establish and operate
21 a National Vetting Center.

22 (b) DIRECTOR.—The Secretary of Homeland Secu-
23 rity shall appoint a senior departmental employee to be
24 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;

1 (4) improve the effectiveness of vetting oper-
2 ations by maximizing the Intelligence Community
3 and law enforcement data holdings used to support
4 vetting;

5 (5) develop and maintain a process to ensure
6 compliance with legal, privacy, and civil rights and
7 civil liberty requirements; and

8 (6) other responsibilities as determined by the
9 Secretary of Homeland Security.

10 **SEC. 213. NATIONAL VETTING GOVERNANCE BOARD.**

11 (a) **ESTABLISHMENT.**—The Secretary of Homeland
12 Security, in coordination with the Secretary of State, the
13 Secretary of Defense, the Attorney General, and the Di-
14 rector of National Intelligence, shall establish a National
15 Vetting Governance Board.

16 (b) **PURPOSE.**—The National Vetting Governance
17 Board shall provide guidance and oversight for the Na-
18 tional Vetting Center established pursuant to section 213
19 of this Act, including—

20 (1) producing decisions and recommendations
21 for unified approaches to and solutions for vetting;

22 (2) recommending a fiscal strategy;

23 (3) recommending priorities for National Vet-
24 ting Center activities;

1 (4) reviewing and recommending new vetting
2 programs or changes to existing vetting activities;

3 (5) reporting progress and making rec-
4 ommendations to Secretary of Homeland Security or
5 their designee; and

6 (6) ensuring National Vetting Governance
7 Board decisions and recommendations are consistent
8 with relevant legal authorities and align with De-
9 partment of Homeland Security privacy, civil rights,
10 and civil liberties policies and practices.

11 (c) LIMITATIONS.—The National Vetting Governance
12 Board is not intended to supersede or otherwise replace
13 existing statutory or delegated roles and responsibilities
14 concerning Department of Homeland Security vetting ac-
15 tivities.

16 (d) OPERATIONS.—

17 (1) The Secretary of Homeland Security, in co-
18 ordination with the Secretary of State, the Secretary
19 of Defense, the Attorney General, and the Director
20 of National Intelligence shall develop the structure,
21 staffing, meeting schedule and other operational
22 issues related to the National Vetting Governance
23 Board.

24 (2) The National Vetting Governance Board
25 shall have a standing privacy and civil liberty work-

1 ing group and a legal working group to review the
2 activities of the National Vetting Center and provide
3 advice to the Board.

4 **Subtitle B—Information Sharing**

5 **SEC. 215. DEPARTMENT OF HOMELAND SECURITY FUSION** 6 **CENTER PARTNERSHIP INITIATIVE.**

7 (a) IN GENERAL.—Section 210A of the Homeland
8 Security Act of 2002 (6 U.S.C. 124h) is amended—

9 (1) by amending the section heading to read as
10 follows:

11 **“SEC. 210A. DEPARTMENT OF HOMELAND SECURITY FU-**
12 **SION CENTER PARTNERSHIP INITIATIVE.”;**

13 (2) in subsection (a), by adding at the end the
14 following: “Beginning on the date of enactment of
15 the Department of Homeland Security Authorization
16 Act, such Initiative shall be known as the ‘Depart-
17 ment of Homeland Security Fusion Center Partner-
18 ship Initiative’.”;

19 (3) by amending subsection (b) to read as fol-
20 lows:

21 **“(b) INTERAGENCY SUPPORT AND COORDINATION.—**
22 **Through the Department of Homeland Security Fusion**
23 **Center Partnership Initiative, in coordination with prin-**
24 **cipal officials of fusion centers in the National Network**
25 **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

1 ensure fusion centers are appropriately aligned with
2 and able to meaningfully support Federal homeland
3 security, national security, and law enforcement ef-
4 forts, including counterterrorism;

5 “(11) encourage the full participation of the
6 National Network of Fusion Centers in all assess-
7 ment and evaluation efforts conducted by the De-
8 partment;

9 “(12) track all Federal funding provided to
10 each fusion center on an individualized basis as well
11 as by funding source;

12 “(13) ensure that none of the departmental in-
13 formation or data provided or otherwise made avail-
14 able to fusion center personnel is improperly dis-
15 seminated, accessed for unauthorized purposes, or
16 otherwise used in a manner inconsistent with De-
17 partment guidance; and

18 “(14) carry out such other duties as the Sec-
19 retary determines appropriate.”;

20 (4) in subsection (c)—

21 (A) in the heading, by striking “PER-
22 SONNEL ASSIGNMENT” and inserting “RE-
23 SOURCE ALLOCATION”;

24 (B) by striking paragraphs (1) and (2) and
25 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

1 may be, by the following Department components
2 and offices, in coordination with the respective com-
3 ponent or office head and in consultation with the
4 principal officials of fusion centers in the National
5 Network of Fusion Centers:

6 “(A) The Office of Intelligence and Anal-
7 ysis.

8 “(B) Cybersecurity and Infrastructure Se-
9 curity Agency.

10 “(C) The Transportation Security Admin-
11 istration.

12 “(D) U.S. Customs and Border Protection.

13 “(E) U.S. Immigration and Customs En-
14 forcement.

15 “(F) The Coast Guard.

16 “(G) The national cybersecurity and com-
17 munications integration center under section
18 2209.

19 “(H) Other components or offices of the
20 Department, as determined by the Secretary.”;

21 (C) in paragraph (3)—

22 (i) in the heading, by striking

23 “QUALIFYING CRITERIA” and inserting

24 “RESOURCE ALLOCATION CRITERIA”; and

1 (ii) by striking subparagraph (A) and
2 inserting the following:

3 “(A) IN GENERAL.—The Secretary shall
4 make available criteria for sharing information
5 and deploying personnel to support a fusion
6 center in the National Network of Fusion Cen-
7 ters in a manner consistent with the Depart-
8 ment’s mission and existing statutory limits.”;
9 and

10 (D) in paragraph (4)(B), in the matter
11 preceding clause (i), by inserting “in which
12 such fusion center is located” after “region”;
13 (5) in subsection (d)—

14 (A) in paragraph (3), by striking “and” at
15 the end;

16 (B) by redesignating paragraph (4) as
17 paragraph (5);

18 (C) by inserting after paragraph (3) the
19 following:

20 “(4) assist, in coordination with the national
21 cybersecurity and communications integration center
22 under section 2209, fusion centers in using informa-
23 tion relating to cybersecurity risks to develop a com-
24 prehensive and accurate threat picture;”;

25 (D) in paragraph (5), as so redesignated—

1 (i) by striking “government” and in-
2 sserting “governments”; and

3 (ii) by striking the period at the end
4 and inserting “; and”; and

5 (E) by adding at the end the following:

6 “(6) use Department information, including in-
7 formation held by components and offices, to develop
8 analysis focused on the mission of the Department
9 under section 101(b).”;

10 (6) in subsection (e)—

11 (A) by amending paragraph (1) to read as
12 follows:

13 “(1) IN GENERAL.—To the greatest extent
14 practicable, the Secretary shall make it a priority to
15 allocate resources, including departmental compo-
16 nent personnel with relevant expertise, to support
17 the efforts of fusion centers along land or maritime
18 borders of the United States to facilitate law en-
19 forcement agency identification, investigation, and
20 interdiction of persons, weapons, and related contra-
21 band that pose a threat to homeland security.”; and

22 (B) in paragraph (2), in the matter pre-
23 ceding subparagraph (A), by striking “partici-
24 pating State, local, and regional fusion centers”

1 and inserting “fusion centers in the National
2 Network of Fusion Centers”;

3 (7) in subsection (j)—

4 (A) by redesignating paragraph (5) as
5 paragraph (7);

6 (B) by redesignating paragraphs (1)
7 through (4) as paragraphs (2) through (5), re-
8 spectively;

9 (C) by inserting before paragraph (2) the
10 following:

11 “(1) the term ‘cybersecurity risk’ has the mean-
12 ing given such term in section 2209;”;

13 (D) in paragraph (5), as so redesignated,
14 by striking “and” at the end; and

15 (E) by inserting after such paragraph (5)
16 the following new paragraph:

17 “(6) the term ‘National Network of Fusion
18 Centers’ means a decentralized arrangement of fu-
19 sion centers intended to enhance individual State
20 and urban area fusion centers’ ability to leverage the
21 capabilities and expertise of all fusion centers for the
22 purpose of enhancing analysis and homeland secu-
23 rity information sharing nationally; and”;

24 (8) by striking subsection (k).

1 (b) REPORT.—Not later than 1 year after the date
2 of the enactment of this Act and annually thereafter
3 through 2024, the Under Secretary for Intelligence and
4 Analysis of the Department of Homeland Security shall
5 report to the Committee on Homeland Security and the
6 Permanent Select Committee on Intelligence of the House
7 of Representatives and the Committee on Homeland Secu-
8 rity and Governmental Affairs and the Select Committee
9 on Intelligence of the Senate on the value of fusion center
10 intelligence products and the expenditure of authorized
11 funds for the support and coordination of the National
12 Network of Fusion Centers as specified in section 210A
13 of the Homeland Security Act of 2002 (6 U.S.C. 124h),
14 as amended by subsection (a).

15 (c) REPORT ON FEDERAL DATABASES.—Not later
16 than 180 days after the date of enactment of this Act,
17 the Comptroller General of the United States shall submit
18 a report to Congress on the Federal databases and
19 datasets that address any gaps identified pursuant to sec-
20 tion 210A(b)(2)(B) of the Homeland Security Act of
21 2002, as amended by subsection (a), including databases
22 and datasets used, operated, or managed by Department
23 components, the Department of Justice, including the
24 Federal Bureau of Investigation and the Drug Enforce-
25 ment Administration, and the Department of the Treas-

1 ury, that are appropriate, in accordance with Federal laws
2 and policies, for inclusion in the information sharing envi-
3 ronment.

4 (d) TECHNICAL AND CONFORMING AMENDMENTS.—

5 (1) Section 2103(c)(1) of the Homeland Secu-
6 rity Act of 2002 (6 U.S.C. 623(c)(1)) is amended by
7 striking “210A(j)(1)” and inserting “210A(j)”.

8 (2) The table of contents in section 1(b) of the
9 Homeland Security Act of 2002 is amended by strik-
10 ing the item relating to section 210A and inserting
11 the following:

“Sec. 210A. Department of Homeland Security Fusion Center Partnership Ini-
tiative.”.

12 (e) REFERENCE.—Any reference in any law, rule, or
13 regulation to the Department of Homeland Security State,
14 Local, and Regional Fusion Center Initiative shall be
15 deemed to be a reference to the Department of Homeland
16 Security Fusion Center Partnership Initiative.

17 **SEC. 216. FUSION CENTER PERSONNEL NEEDS ASSESS-**
18 **MENT.**

19 (a) ASSESSMENT.—

20 (1) IN GENERAL.—Not later than 240 days
21 after the date of the enactment of this Act, the
22 Comptroller General of the United States shall con-
23 duct an assessment of Department of Homeland Se-
24 curity personnel assigned to fusion centers pursuant

1 to section 210A(c) of the Homeland Security Act of
2 2002 (6 U.S.C. 124h(c)), as amended by this title,
3 including an assessment of whether deploying addi-
4 tional Department personnel to such fusion centers
5 would enhance the Department's mission under sec-
6 tion 101(b) of such Act (6 U.S.C. 111(b)) and the
7 National Network of Fusion Centers.

8 (2) CONTENTS.—The assessment required
9 under this subsection shall include the following:

10 (A) Information on the current deployment
11 of the Department's personnel to each fusion
12 center.

13 (B) Information on the roles and respon-
14 sibilities of the Department's Office of Intel-
15 ligence and Analysis intelligence officers, intel-
16 ligence analysts, senior reports officers, reports
17 officers, and regional directors deployed to fu-
18 sion centers.

19 (C) Information on Federal resources, in
20 addition to personnel, provided to each fusion
21 center.

22 (D) An analysis of the optimal number of
23 personnel the Office of Intelligence and Anal-
24 ysis should deploy to fusion centers, including a
25 cost-benefit analysis comparing deployed per-

1 sonnel with technological solutions to support
2 information sharing.

3 (E) An assessment of fusion centers lo-
4 cated in jurisdictions along land and maritime
5 borders of the United States, and the degree to
6 which deploying personnel, as appropriate, from
7 U.S. Customs and Border Protection, U.S. Im-
8 migration and Customs Enforcement, and the
9 Coast Guard to such fusion centers would en-
10 hance the integrity and security at such borders
11 by helping Federal, State, local, Tribal, and ter-
12 ritorial law enforcement authorities to identify,
13 investigate, and interdict persons, weapons, and
14 related contraband that pose a threat to home-
15 land security.

16 (F) An assessment of fusion centers lo-
17 cated in jurisdictions with large and medium
18 hub airports, and the degree to which deploy-
19 ing, as appropriate, personnel from the Trans-
20 portation Security Administration to such fu-
21 sion centers would enhance the integrity and se-
22 curity of aviation security.

23 (b) DEFINITIONS.—In this section, the terms “fusion
24 center” and “National Network of Fusion Centers” have
25 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

1 U.S.C. 3161 note) to sponsor Top Secret clearances
2 for appropriate State, local, Tribal, and territorial
3 analysts located in fusion centers.

4 (2) The effects of such Top Secret clearances
5 on enhancing information sharing with State, local,
6 Tribal, and territorial partners.

7 (3) The cost for providing such Top Secret
8 clearances for State, local, Tribal, and territorial an-
9 alysts located in fusion centers, including training
10 and background investigations.

11 (4) The operational security protocols, training,
12 management, and risks associated with providing
13 such Top Secret clearances for State, local, Tribal,
14 and territorial analysts located in fusion centers.

15 (c) DEFINITION.—In this section, the term “fusion
16 center” has the meaning given the term in section 210A(j)
17 of the Homeland Security Act of 2002 (6 U.S.C. 124h(j)),
18 as amended by this title.

19 **SEC. 218. INFORMATION TECHNOLOGY ASSESSMENT.**

20 (a) IN GENERAL.—The Under Secretary for Intel-
21 ligence and Analysis of the Department of Homeland Se-
22 curity, in collaboration with the Chief Information Officer
23 of the Department of Homeland Security and representa-
24 tives from the National Network of Fusion Centers, shall
25 conduct an assessment of information systems used to

1 share homeland security information between the Depart-
2 ment of Homeland Security and fusion centers in the Na-
3 tional Network of Fusion Centers and make upgrades to
4 such systems, as appropriate. Such assessment shall in-
5 clude the following:

6 (1) An evaluation of the security, accessibility,
7 and ease of use of such systems by fusion centers in
8 the National Network of Fusion Centers.

9 (2) A review to determine how to establish im-
10 proved interoperability of departmental information
11 systems with existing information systems used by
12 fusion centers in the National Network of Fusion
13 Centers.

14 (3) An evaluation of participation levels of de-
15 partmental components and offices of information
16 systems used to share homeland security information
17 with fusion centers in the National Network of Fu-
18 sion Centers.

19 (b) DEFINITIONS.—In this section—

20 (1) the terms “fusion center” and “National
21 Network of Fusion Centers” have the meanings
22 given those terms in section 210A(j) of the Home-
23 land Security Act of 2002 (6 U.S.C. 124h(j)), as
24 amended by this title;

1 (2) the term “homeland security information”
2 has the meaning given the term in section 892 of the
3 Homeland Security Act of 2002 (6 U.S.C. 482); and

4 (3) the term “information systems” has the
5 meaning given the term in section 3502 of title 44,
6 United States Code.

7 **SEC. 219. DEPARTMENT OF HOMELAND SECURITY CLASSI-**
8 **FIED FACILITY INVENTORY AND DISSEMINA-**
9 **TION.**

10 (a) IN GENERAL.—The Secretary of Homeland Secu-
11 rity shall, to the extent practicable—

12 (1) maintain an inventory of those Department
13 of Homeland Security facilities that the Department
14 certifies to house classified infrastructure or systems
15 at the Secret level and above;

16 (2) update such inventory on a regular basis;
17 and

18 (3) share part or all of such inventory with ap-
19 propriate departmental personnel and representa-
20 tives of other Federal, State, and local agencies as
21 determined appropriate by the Secretary of Home-
22 land Security.

23 (b) INVENTORY.—The inventory of facilities de-
24 scribed in subsection (a) may include—

25 (1) the location of such facilities;

1 (2) the attributes and capabilities of such facili-
2 ties (including the clearance level of the facility, the
3 square footage of, the total capacity of, the number
4 of workstations in, document storage, and the num-
5 ber of conference rooms in, such facilities);

6 (3) the entities that operate such facilities; and

7 (4) the date of establishment of such facilities.

8 **SEC. 220. TERROR INMATE INFORMATION SHARING.**

9 (a) IN GENERAL.—The Secretary of Homeland Secu-
10 rity, in coordination with the Attorney General and in con-
11 sultation with other appropriate Federal officials, shall, as
12 appropriate, share with State, local, and regional fusion
13 centers through the Department of Homeland Security
14 Fusion Center Partnership Initiative under section 210A
15 of the Homeland Security Act of 2002 (6 U.S.C. 124h),
16 as well as other relevant law enforcement entities, release
17 information from a Federal correctional facility, including
18 the name, charging date, and expected place and date of
19 release, of certain individuals who may pose a terrorist
20 threat.

21 (b) SCOPE.—The information shared pursuant to
22 subsection (a) shall be—

23 (1) for homeland security purposes; and

24 (2) regarding individuals convicted of a Federal
25 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.

1 **SEC. 221. ENHANCING DEPARTMENT OF HOMELAND SECU-**
2 **RITY SUSPICIOUS ACTIVITY REPORTING OP-**
3 **ERATIONS.**

4 (a) STRATEGY REQUIRED.—Not later than one year
5 after the date of the enactment of this Act, the Secretary
6 of Homeland Security, in consultation with other appro-
7 priate officials, shall develop a strategy to improve the op-
8 erations and activities of the Department of Homeland Se-
9 curity related to training, outreach, and information shar-
10 ing for suspicious activity reporting to prevent acts of ter-
11 rorism and acts of targeted violence.

12 (b) CONTENTS OF STRATEGY.—The strategy re-
13 quired under subsection (a) shall include the following:

14 (1) A plan to maintain and expand activities re-
15 lated to effectively identifying, reporting, and re-
16 sponding to potential acts of terrorism.

17 (2) A plan to develop a behavioral threat as-
18 sessment and management model for use by appro-
19 priate National Network of Fusion Centers, emer-
20 gency response providers, and appropriate private
21 sector personnel involved in reporting or responding
22 suspicious activity related to acts of targeted vio-
23 lence.

24 (3) Protocols, developed in consultation with
25 the Federal Bureau of Investigation, to ensure that

1 the Federal Bureau of Investigations receives all rel-
2 evant suspicious activity reports.

3 (4) A staffing and budget plan to ensure the
4 continued operation and any necessary expansion of
5 Department of Homeland Security information shar-
6 ing, technical assistance, training, and other activi-
7 ties related to suspicious activity reporting.

8 (5) Training for appropriate personnel of the
9 National Network of Fusion Centers, emergency re-
10 sponse providers, and appropriate private sector per-
11 sonnel on—

12 (A) methods for identifying, analyzing, and
13 disseminating critical information, including the
14 indicators of acts of terrorism and acts of tar-
15 geted violence;

16 (B) methods to protect privacy and civil
17 liberties, including preventing racial, religious,
18 and national origin discrimination;

19 (C) implementation of the behavioral
20 threat assessment and management model;

21 (D) response protocols for submitting sus-
22 picious activity reports; and

23 (E) other training determined appropriate
24 by the Secretary.

25 (6) A plan to—

1 (A) provide technical assistance for appro-
2 priate National Network of Fusion Centers,
3 emergency response providers, and appropriate
4 private sector personnel for operations related
5 to suspicious activity reporting activity; and

6 (B) assist with questions or concerns re-
7 lated to privacy and civil liberty protections.

8 (c) CONGRESSIONAL NOTIFICATION.—The Secretary
9 shall provide to the Committee on Homeland Security of
10 the House of Representatives and the Committee on
11 Homeland Security and Governmental Affairs of the Sen-
12 ate a copy of the strategy required in subsection (a).

13 (d) DEFINITIONS.—In this section:

14 (1) BEHAVIORAL THREAT ASSESSMENT.—The
15 term “behavioral threat assessment and manage-
16 ment” means the systematic and evidence-based
17 process of—

18 (A) identifying individuals who are exhib-
19 iting patterns of concerning behavior that indi-
20 cate an interest, motive, intention, or capability
21 of carrying out an act of violence;

22 (B) investigating and gathering informa-
23 tion from multiple sources to assess whether an
24 individual described in subparagraph (A) poses
25 a threat, based on articulable facts; and

1 (C) the subsequent management of such a
2 threat, if necessary.

3 (2) EMERGENCY RESPONSE PROVIDERS.—The
4 term “emergency response provider” has the mean-
5 ing given such term in section 2(6) of the Homeland
6 Security Act.

7 (3) NATIONAL NETWORK OF FUSION CEN-
8 TERS.—The term “National Network of Fusion Cen-
9 ters” has the meaning given such term in section
10 215 of this Act.

11 (4) TARGETED VIOLENCE.—The term “targeted
12 violence” means any incident of predatory violence
13 with respect to which an identifiable individual or
14 group focuses an attack on a particular target.

15 (5) TERRORISM.—The term “terrorism” has
16 the meaning given such term in section 2331 of title
17 18, United States Code.

18 **TITLE III—CYBERSECURITY**

19 **SEC. 301. CYBERSECURITY ADVISORY COMMITTEE.**

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

1 **“SEC. 2215. CYBERSECURITY ADVISORY COMMITTEE.**

2 “(a) ESTABLISHMENT.—The Secretary shall estab-
3 lish within the Cybersecurity and Infrastructure Security
4 Agency a Cybersecurity Advisory Committee.

5 “(b) DUTIES.—

6 “(1) IN GENERAL.—The Advisory Committee
7 may advise, consult with, report to, and make rec-
8 ommendations to the Director of Cybersecurity and
9 Infrastructure Security on the development, refine-
10 ment, and implementation of policies, programs,
11 rulemakings, planning, training, and security direc-
12 tives pertaining to the mission of the Cybersecurity
13 and Infrastructure Security Agency.

14 “(2) RECOMMENDATIONS.—

15 “(A) IN GENERAL.—The Advisory Com-
16 mittee shall develop, at the request of the Di-
17 rector, recommendations for improvements to
18 the cybersecurity mission of the Cybersecurity
19 and Infrastructure Security Agency.

20 “(B) RECOMMENDATIONS OF SUBCOMMIT-
21 TEES.—Recommendations agreed upon by the
22 subcommittees established under subsection (d)
23 for any year shall be approved by the Advisory
24 Committee before the Advisory Committee sub-
25 mits to the Director the annual report under
26 paragraph (4) for that year.

1 “(3) PERIODIC REPORTS.—The Advisory Com-
2 mittee shall periodically submit to the Director—

3 “(A) reports on matters identified by the
4 Director; and

5 “(B) reports on other matters identified by
6 a majority of the members of the Advisory
7 Committee.

8 “(4) ANNUAL REPORT.—The Advisory Com-
9 mittee shall submit to the Director an annual report
10 providing information on the activities, findings, and
11 recommendations of the Advisory Committee, includ-
12 ing its subcommittees, for the preceding year. Not
13 later than six months after the date that the Direc-
14 tor receives an annual report for a year, the Director
15 shall publish a public version of the report describ-
16 ing the activities of the Advisory Committee and
17 such related matters as would be informative to the
18 public during that year, consistent with section
19 552(b) of title 5, United States Code.

20 “(5) FEEDBACK.—Not later than 90 days after
21 receiving any recommendation submitted by the Ad-
22 visory Committee under paragraph (2), (3), or (4),
23 the Director shall respond in writing to the Advisory
24 Committee with feedback on the recommendation.
25 Such a response shall include—

1 “(A) with respect to any recommendation
2 with which the Director concurs, an action plan
3 to implement the recommendation; and

4 “(B) with respect to any recommendation
5 with which the Director does not concur, a jus-
6 tification for why the Director does not plan to
7 implement the recommendation.

8 “(6) CONGRESSIONAL NOTIFICATION.—For
9 each fiscal quarter beginning after the date of the
10 enactment of this section, the Director shall provide
11 to the Committee on Homeland Security and Gov-
12 ernmental Affairs and the Committee on Appropria-
13 tions of the Senate and the Committee on Homeland
14 Security and the Committee on Appropriations of
15 the House of Representatives a briefing on feedback
16 from the Advisory Committee.

17 “(c) MEMBERSHIP.—

18 “(1) APPOINTMENT.—

19 “(A) IN GENERAL.—Not later than 180
20 days after the date of the enactment of this
21 Act, the Director shall appoint the members of
22 the Advisory Committee.

23 “(B) COMPOSITION.—The membership of
24 the Advisory Committee shall consist of not
25 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.—

1 “(A) IN GENERAL.—The Director shall re-
2 quire the Advisory Committee to meet at least
3 quarterly, and may convene additional meetings
4 as necessary.

5 “(B) PUBLIC MEETINGS.—At least one of
6 the meetings referred to in subparagraph (A)
7 shall be open to the public.

8 “(C) ATTENDANCE.—The Advisory Com-
9 mittee shall maintain a record of the persons
10 present at each meeting.

11 “(6) MEMBER ACCESS TO CLASSIFIED AND
12 PROTECTED INFORMATION.—

13 “(A) IN GENERAL.—Not later than 60
14 days after the date on which a member is first
15 appointed to the Advisory Committee and be-
16 fore the member is granted access to any classi-
17 fied information or protected information, the
18 Director shall determine if there is cause for
19 such member to be restricted from reviewing,
20 discussing, or possessing such information.

21 “(B) ACCESS.—

22 “(i) PROTECTED INFORMATION.—If
23 the Director does not restrict a member
24 from reviewing, discussing, or possessing
25 sensitive information under subparagraph

1 (A) and the member voluntarily signs a
2 nondisclosure agreement with respect to
3 protected information, the member may be
4 granted access to protected information
5 that the Director determines is relevant to
6 such member's service on the Advisory
7 Committee.

8 (ii) CLASSIFIED INFORMATION.—Ac-
9 cess to classified materials shall be man-
10 aged in accordance with Executive Order
11 No. 13526 of December 29, 2009 (75 Fed.
12 Reg 707), or any subsequent corresponding
13 Executive Order.

14 (C) PROTECTIONS.—A member of the
15 Advisory Committee shall agree, as a condition
16 of such membership, to protect all classified in-
17 formation in accordance with the applicable re-
18 quirements for the particular level of classifica-
19 tion of such information and to protect all pro-
20 tected information appropriately.

21 (D) PROTECTED INFORMATION DE-
22 FINED.—In this section, the term 'protected in-
23 formation' means—

24 (i) information specifically exempted
25 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 addition to the subcommittees established pursuant to paragraph (1), the Advisory Committee chairperson, in coordination with the Director, may establish within the Advisory Committee additional subcommittees that the Director and Advisory Committee determine to be necessary.

12 “(3) MEETINGS AND REPORTING.—Each subcommittee shall meet at least bimonthly, and submit to the Advisory Committee for inclusion in the annual report required under subsection (b)(4) information, including activities, findings, and recommendations, regarding subject matter considered by the subcommittee.

19 “(4) SUBJECT MATTER EXPERTS.—The chair of the Advisory Committee shall appoint members to subcommittees and shall ensure that each member appointed to a subcommittee has subject matter expertise relevant to the subject matter of the subcommittee.

1 “(e) NONAPPLICABILITY OF FACA.—The Federal
2 Advisory Committee Act (5 U.S.C. App.) shall not apply
3 to the Advisory Committee and its subcommittees.”.

4 (b) CLERICAL AMENDMENT.—The table of contents
5 in section 1(b) of such Act is amended by inserting after
6 the item relating to section 2214 the following new item:

“Sec. 2215. Cybersecurity Advisory Committee.”.

7 **SEC. 302. CYBERSECURITY ESSENTIALS.**

8 (a) IN GENERAL.—Subsection (b) of section 2203 of
9 the Homeland Security act of 2002 (6 U.S.C. 653) is
10 amended—

11 (1) in paragraph (3), by striking “and” after
12 the semicolon at the end;

13 (2) by redesignating paragraph (4) as para-
14 graph (5); and

15 (3) by inserting after paragraph (3) the fol-
16 lowing new paragraph:

17 “(4) develop, publish and update as necessary
18 guidelines and processes for a national audience re-
19 garding best practices for effective and usable basic
20 controls that have the most impact in defending
21 again common cybersecurity threats and cybersecu-
22 rity risks; and”.

23 (b) RESTRICTION.—Chapter 35 of title 44, United
24 States Code (commonly known as the “Paperwork Reduc-

1 tion Act”) shall not apply to any action to implement this
2 Act.

3 **SEC. 303. ESTABLISHMENT OF CONTINUOUS DIAGNOSTICS**
4 **AND MITIGATION PROGRAM IN THE CYBER-**
5 **SECURITY AND INFRASTRUCTURE SECURITY**
6 **AGENCY.**

7 (a) IN GENERAL.—Section 2213 of the Homeland
8 Security Act of 2002 (6 U.S.C. 663) is amended by adding
9 at the end the following new subsection:

10 “(g) CONTINUOUS DIAGNOSTICS AND MITIGATION.—

11 “(1) PROGRAM.—

12 “(A) IN GENERAL.—The Secretary, acting
13 through the Director of Cybersecurity and In-
14 frastructure Security, shall deploy, operate, and
15 maintain a continuous diagnostics and mitiga-
16 tion program for agencies. Under such pro-
17 gram, the Secretary shall—

18 “(i) assist agencies to continuously di-
19 agnose and mitigate cyber threats and
20 vulnerabilities;

21 “(ii) develop and provide the capa-
22 bility to collect, analyze, and visualize in-
23 formation relating to security data and cy-
24 bersecurity 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

1 and in real time, provide to the Secretary all infor-
2 mation, assessments, analyses, and raw data col-
3 lected by the program, in a manner specified by the
4 Secretary.

5 “(3) RESPONSIBILITIES OF THE SECRETARY.—
6 In carrying out the continuous diagnostics and miti-
7 gation program under paragraph (1), the Secretary
8 shall, as appropriate—

9 “(A) share with agencies relevant analysis
10 and products developed under such program;

11 “(B) provide regular reports on cybersecu-
12 rity risks to agencies; and

13 “(C) provide comparative assessments of
14 cybersecurity risks for agencies.”.

15 (b) CONTINUOUS DIAGNOSTICS AND MITIGATION
16 STRATEGY.—

17 (1) IN GENERAL.—Not later than 180 days
18 after the date of the enactment of this Act, the Sec-
19 retary of Homeland Security shall develop a com-
20 prehensive continuous diagnostics and mitigation
21 strategy to carry out the continuous diagnostics and
22 mitigation program required under subsection (g) of
23 section 2213 of the Homeland Security Act of 2002
24 (6 U.S.C. 663), as added by subsection (a).

1 (2) SCOPE.—The strategy required under para-
2 graph (1) shall include the following:

3 (A) A description of the continuous
4 diagnostics and mitigation program, including
5 efforts by the Secretary of Homeland Security
6 to assist with the deployment of program tools,
7 capabilities, and services, from the inception of
8 the program referred to in paragraph (1) to the
9 date of enactment of this Act.

10 (B) A description of the coordination and
11 funding required to deploy, install, and main-
12 tain the tools, capabilities, and services that the
13 Secretary of Homeland Security determines to
14 be necessary to satisfy the requirements of such
15 program.

16 (C) A description of any obstacles facing
17 the deployment, installation, and maintenance
18 of tools, capabilities, and services under such
19 program.

20 (D) Recommendations and guidelines to
21 help maintain and continuously upgrade tools,
22 capabilities, and services provided under such
23 program.

24 (E) Recommendations for using the data
25 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).

1 (d) GAO REPORT.—Not later than 1 year after the
2 date of enactment of this Act, the Comptroller General
3 of the United States shall submit a report to Congress
4 on the potential impacts and benefits of replacing the re-
5 porting requirements under chapter 35 of title 44, United
6 States Code, with periodical real-time data provided by the
7 continuous diagnostics and mitigation program under sub-
8 section (g) of section 2213 of the Homeland Security Act
9 of 2002 (6 U.S.C. 663), as added by subsection (a).

10 **SEC. 304. ADMINISTRATIVE SUBPOENA AUTHORITY.**

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

13 (1) in subsection (a)—

14 (A) by redesignating paragraph (6) as
15 paragraph (7); and

16 (B) by inserting after paragraph (5) the
17 following:

18 “(6) the term ‘security vulnerability’ has the
19 meaning given that term in section 102(17) of the
20 Cybersecurity Information Sharing Act of 2015 (615
21 U.S.C. 1501(17));”;

22 (2) in subsection (c)—

23 (A) in paragraph (10), by striking “and”
24 at the end;

1 (B) in paragraph (11), by striking the pe-
2 riod at the end and inserting “; and”; and

3 (C) by adding at the end the following:

4 “(12) detecting, identifying, and receiving infor-
5 mation about security vulnerabilities relating to crit-
6 ical infrastructure in the information systems and
7 devices of Federal and non-Federal entities for a cy-
8 bersecurity purpose, as defined in section 102 of the
9 Cybersecurity Information Sharing Act of 2015 (6
10 U.S.C. 1501), and notifying the owners and opera-
11 tors of critical infrastructure with such security vul-
12 nerability.”; and

13 (3) by adding at the end the following:

14 “(n) SUBPOENA AUTHORITY.—

15 “(1) DEFINITION.—In this subsection, the term
16 ‘enterprise device or system’—

17 “(A) means a device or system commonly
18 used to perform industrial, commercial, sci-
19 entific, or governmental functions or processes
20 that relate to critical infrastructure, including
21 operational and industrial control systems, dis-
22 tributed control systems, and programmable
23 logic controllers; and

24 “(B) does not include personal devices and
25 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

1 apply to any subpoena issued under the author-
2 ity under subparagraph (A).

3 “(3) COORDINATION.—

4 “(A) IN GENERAL.—If the Director decides
5 to exercise the subpoena authority under this
6 subsection, and in the interest of avoiding inter-
7 ference with ongoing law enforcement investiga-
8 tions, the Director shall coordinate the issuance
9 of any such subpoena with the Department of
10 Justice, including the Federal Bureau of Inves-
11 tigation, pursuant to inter-agency procedures
12 which the Director, in coordination with the At-
13 torney General, shall develop not later than 60
14 days after the date of enactment of this sub-
15 section.

16 “(B) CONTENTS.—The inter-agency proce-
17 dures developed under this paragraph shall pro-
18 vide that a subpoena issued by the Director
19 under this subsection shall be—

20 “(i) issued in order to carry out a
21 function described in subsection (c)(12);
22 and

23 “(ii) subject to the limitations under
24 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-

1 quest, providing other resources to parties or
2 entities to prevent a recurrence of the vulner-
3 ability or a related vulnerability in the future.

4 “(9) REVIEW OF PROCEDURES.—Not later than
5 1 year after the date of enactment of this sub-
6 section, the Privacy Officer of the Agency shall—

7 “(A) review the procedures developed by
8 the Director under paragraph (8) to ensure
9 that—

10 “(i) the procedures are consistent with
11 fair information practices; and

12 “(ii) the operations of the Agency
13 comply with the procedures; and

14 “(B) notify the Committee on Homeland
15 Security and Governmental Affairs of the Sen-
16 ate and the Committee on Homeland Security
17 of the House of Representatives of the results
18 of the review.

19 “(10) PUBLICATION OF INFORMATION.—Not
20 later than 120 days after establishing the internal
21 procedures under paragraph (8), the Director shall
22 make publicly available information regarding the
23 subpoena process under this subsection, including
24 regarding—

1 “(A) the purpose for subpoenas issued
2 under this subsection;

3 “(B) the subpoena process;

4 “(C) the criteria for the critical infrastruc-
5 ture security risk assessment conducted prior to
6 issuing a subpoena;

7 “(D) policies and procedures on retention
8 and sharing of data obtained by subpoena;

9 “(E) guidelines on how entities contacted
10 by the Director may respond to notice of a sub-
11 poena; and

12 “(F) the procedures and policies of the
13 Agency developed under paragraph (8).

14 “(11) ANNUAL REPORTS.—The Director shall
15 annually submit to the Committee on Homeland Se-
16 curity and Governmental Affairs of the Senate and
17 the Committee on Homeland Security of the House
18 of Representatives a report (which may include a
19 classified annex but with the presumption of declas-
20 sification) on the use of subpoenas under this sub-
21 section by the Director, which shall include—

22 “(A) a discussion of—

23 “(i) the effectiveness of the use of
24 subpoenas to mitigate critical infrastruc-
25 ture 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

1 resolution or mitigation of the critical in-
2 frastructure security vulnerability.

3 “(12) PUBLICATION OF THE ANNUAL RE-
4 PORTS.—The Director shall make a version of the
5 annual report required by paragraph (11) publicly
6 available, which shall, at a minimum, include the
7 findings described in clause (iii), (iv) and (v) of sub-
8 paragraph (A).”.

9 **SEC. 305. CISA DIRECTOR TERM LIMITATION.**

10 (a) IN GENERAL.—Subsection (b) of section 2202 of
11 the Homeland Security Act of 2002 (6 U.S.C. 652) is
12 amended by—

13 (1) redesignating paragraph (2) as paragraph
14 (3); and

15 (2) inserting after paragraph (1) the following
16 new paragraph:

17 “(2) TERM.—Effective with respect to an indi-
18 vidual appointed to be the Director by the President,
19 by and with the advice and consent of the Senate,
20 after the date of the enactment of this paragraph,
21 the term of office of such an individual so appointed
22 shall be five years, and such an individual may not
23 serve more than two terms. The term of office of the
24 individual serving as the Director as of such date of

1 enactment shall be five years beginning on the date
2 on which the Director began serving.”.

3 (b) AMENDMENT RELATING TO QUALIFICATIONS
4 FOR CERTAIN CISA ASSISTANT DIRECTORS.—The Home-
5 land Security Act of 2002 is amended—

6 (1) in subparagraph (B) of section 2203(a)(2)
7 (6 U.S.C. 653(a)(2)), by striking “President without
8 the advice and consent of the Senate” and inserting
9 “Secretary”; and

10 (2) in subparagraph (B) of section 2204(a)(2)
11 (6 U.S.C. 654(a)(2)), by striking “President without
12 the advice and consent of the Senate” and inserting
13 “Secretary”.

14 (c) AMENDMENT TO POSITION LEVEL OF CISA DI-
15 RECTOR.—Subchapter II of chapter 53 of title 5, United
16 States Code, is amended—

17 (1) in section 5313, by inserting after “Admin-
18 istrator of the Transportation Security Administra-
19 tion.” the following:

20 “Director, Cybersecurity and Infrastructure Se-
21 curity Agency.”; and

22 (2) in section 5314, by striking “Director, Cy-
23 bersecurity and Infrastructure Security Agency.”.

1 **SEC. 306. STATE, LOCAL, TRIBAL AND TERRITORIAL CY-**
2 **BERSECURITY.**

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

7 **“SEC. 2216. CYBERSECURITY RESOURCE GUIDE DEVELOP-**
8 **MENT FOR STATE, AND LOCAL, TRIBAL, AND**
9 **TERRITORIAL GOVERNMENT OFFICIALS.**

10 “The Secretary, acting through the Director, shall
11 develop a resource guide for use by State, local, and Tribal
12 officials, including law enforcement officers, to help such
13 officials prepare for, protect against, respond to, recover
14 from, and mitigate against cyber attacks.

15 **“SEC. 2217. STATE, LOCAL, TRIBAL, AND TERRITORIAL CY-**
16 **BERSECURITY GRANTS.**

17 “(a) IN GENERAL.—The Director shall establish a
18 State, local, Tribal, and territorial government cybersecu-
19 rity initiative to make grants to State, local, Tribal, and
20 territorial governments to prepare for, protect against, re-
21 spond to, recover from, and mitigate against cyber at-
22 tacks.

23 “(b) APPLICATION.—

24 “(1) IN GENERAL.—Each State, local, Tribal,
25 and territorial government may apply for a grant
26 under this section, and shall submit such informa-

1 tion in support of an application relating thereto as
2 the Director may require.

3 “(2) MINIMUM CONTENTS OF APPLICATION.—

4 An application under this subsection shall include
5 the following:

6 “(A) A description of how the State, local,
7 Tribal, or territorial government plans to allo-
8 cate grant funds.

9 “(B) A budget showing how the State,
10 local, Tribal, or territorial government intends
11 to expend grant funds.

12 “(3) DURATION.—Grants under this section
13 shall be for one year, and a State, local, Tribal, or
14 territorial government may apply or reapply on an
15 annual basis.

16 “(c) GRANT AWARD.—To be eligible to receive a
17 grant under this section, a State, local, Tribal, or terri-
18 torial government shall agree to contribute, from State or
19 local government appropriated funds, other State or local
20 government revenue, or from private contributions re-
21 ceived by the State or local government, not less than 20
22 percent of the amount of the grant.

23 “(d) AUTHORIZATION OF APPROPRIATIONS.—There
24 is authorized to be appropriated \$50,000,000 for each of
25 fiscal years 2020 through 2024 and such sums as may

1 be necessary for each fiscal year thereafter to carry out
2 this section.”.

3 (b) CLERICAL AMENDMENT.—The table of contents
4 in section 1(b) of the Homeland Security Act of 2002 is
5 amended by inserting after the item relating to section
6 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.”.

7 (c) ADDITIONAL REQUIREMENTS.—Subtitle A of title
8 XXII of the Homeland Security Act of 2002 (6 U.S.C 652
9 et seq.), as amended by this title, is further amended—
10 (1) in section 2201 (6 U.S.C. 651)—

11 (A) by redesignating paragraphs (4), (5),
12 and (6) as paragraphs (5), (6), and (7), respec-
13 tively; and

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

16 “(4) ENTITY.—The term ‘entity’ shall in-
17 clude—

18 “(A) an association, corporation, whether
19 for-profit or nonprofit, partnership, proprietor-
20 ship, organization, institution, establishment, or
21 individual, whether domestic or foreign;

22 “(B) a government agency or other govern-
23 mental entity, whether domestic or foreign, in-

1 including 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 cyberse-
13 curity 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-

1 security standards and best practices related to infor-
2 mation security, including by, as appropriate, de-
3 ploying and sustaining cybersecurity technologies,
4 such as an intrusion detection capability, to assist
5 such Federal and non-Federal entities in detecting
6 cybersecurity risks and incidents;

7 “(8) assist Federal and non-Federal entities in
8 developing policies and procedures for coordinating
9 vulnerability disclosures, to the extent practicable,
10 consistent with international and national standards
11 in the information technology industry;

12 “(9) ensure that Federal and non-Federal enti-
13 ties, as appropriate, are made aware of the tools,
14 products, resources, policies, guidelines, controls,
15 procedures, and other cybersecurity standards and
16 best practices related to information security devel-
17 oped by the Department and other appropriate Fed-
18 eral entities for ensuring the security and resiliency
19 of civilian information systems; and

20 “(10) promote cybersecurity education and
21 awareness through engagements with Federal and
22 non-Federal entities.”.

23 **SEC. 307. CYBERSECURITY WORKFORCE.**

24 (a) **CYBERSECURITY TALENT EXCHANGE.—**

25 (1) **DEFINITIONS.—**In this section—

1 (A) the term “congressional homeland se-
2 curity committees” means—

3 (i) the Committee on Homeland Secu-
4 rity and Governmental Affairs and the
5 Committee on Appropriations of the Sen-
6 ate; and

7 (ii) the Committee on Homeland Se-
8 curity and the Committee on Appropria-
9 tions of the House of Representatives;

10 (B) the term “Department” means the De-
11 partment of Homeland Security; and

12 (C) the term “Secretary” means the Sec-
13 retary of Homeland Security.

14 (2) CYBERSECURITY TALENT EXCHANGE PILOT
15 PROGRAM.—

16 (A) IN GENERAL.—Not later than 1 year
17 after the date of enactment of this Act, the Sec-
18 retary shall commence carrying out a cybersecu-
19 rity talent exchange pilot program.

20 (B) DELEGATION.—The Secretary may
21 delegate any authority under this section to the
22 Director of the Cybersecurity and Infrastruc-
23 ture Security Agency of the Department.

24 (3) APPOINTMENT AUTHORITY.—

1 (A) IN GENERAL.—Under regulations pre-
2 scribed by the Secretary for the purpose of car-
3 rying out the pilot program established under
4 subsection (b), the Secretary may, with the
5 agreement of a private-sector organization and
6 the consent of the employee, arrange for the
7 temporary assignment of an employee to the
8 private-sector organization, or from the private-
9 sector organization to a Department organiza-
10 tion under this section.

11 (B) ELIGIBLE EMPLOYEES.—Employees
12 participating in the pilot program established
13 under subsection (b) shall have significant edu-
14 cation, skills, or experience relating to cyberse-
15 curity.

16 (C) AGREEMENTS.—

17 (i) IN GENERAL.—The Secretary shall
18 provide for a written agreement among the
19 Department, the private-sector organiza-
20 tion, and the employee concerned regard-
21 ing the terms and conditions of the assign-
22 ment of the employee under this section,
23 which—

24 (I) shall require that the em-
25 ployee 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

1 (IV) shall cover matters relating
2 to confidentiality, intellectual property
3 rights, and such other matters as the
4 Secretary considers appropriate.

5 (ii) LIABILITY.—An amount for which
6 an employee is liable under subparagraph
7 (i)(II) shall be treated as a debt due the
8 United States.

9 (iii) WAIVER.—The Secretary may
10 waive, in whole or in part, collection of a
11 debt described in subparagraph (B) based
12 on a determination that the collection
13 would be against equity and good con-
14 science and not in the best interests of the
15 United States, after taking into account
16 any indication of fraud, misrepresentation,
17 fault, or lack of good faith on the part of
18 the employee.

19 (D) TERMINATION.—An assignment under
20 this subsection may, at any time and for any
21 reason, be terminated by the Department or the
22 private-sector organization concerned.

23 (E) DURATION.—

24 (i) IN GENERAL.—Except as provided
25 in subparagraph (B), an assignment under

1 this subsection shall be for a period of not
2 less than 3 months and not more than 2
3 years, and renewable up to a total of 4
4 years.

5 (ii) EXCEPTION.—An assignment
6 under this subsection may be for a period
7 in excess of 2 years, but not more than 4
8 years, if the Secretary determines that the
9 assignment is necessary to meet critical
10 mission or program requirements.

11 (iii) LIMITATION.—No employee of
12 the Department may be assigned under
13 this subsection for more than a total of 4
14 years inclusive of all assignments.

15 (F) STATUS OF FEDERAL EMPLOYEES AS-
16 SIGNED TO PRIVATE-SECTOR ORGANIZATIONS.—

17 (i) IN GENERAL.—An employee of the
18 Department who is assigned to a private-
19 sector organization under this subsection
20 shall be considered, during the period of
21 assignment, to be on detail to a regular
22 work assignment in the Department for all
23 purposes.

24 (ii) WRITTEN AGREEMENT.—The
25 written agreement established under para-

1 graph (3) shall address the specific terms
2 and conditions related to the continued
3 status of the employee as a Federal em-
4 ployee.

5 (iii) CERTIFICATION.—In establishing
6 a temporary assignment of an employee of
7 the Department to a private-sector organi-
8 zation, the Secretary shall—

9 (I) ensure that the normal duties
10 and functions of the employee can be
11 reasonably performed by other em-
12 ployees of the Department without the
13 transfer or reassignment of other per-
14 sonnel of the Department; and

15 (II) certify that the temporary
16 assignment of the employee shall not
17 have an adverse or negative impact on
18 organizational capabilities associated
19 with the assignment.

20 (G) TERMS AND CONDITIONS FOR PRI-
21 VATE-SECTOR EMPLOYEES.—An employee of a
22 private-sector organization who is assigned to a
23 Department organization under this sub-
24 section—

1 (i) shall continue to receive pay and
2 benefits from the private-sector organiza-
3 tion from which the employee is assigned
4 and shall not receive pay or benefits from
5 the Department, except as provided in sub-
6 paragraph (B);

7 (ii) is deemed to be an employee of
8 the Department for the purposes of—

9 (I) chapters 73 and 81 of title 5,
10 United States Code;

11 (II) sections 201, 203, 205, 207,
12 208, 209, 603, 606, 607, 643, 654,
13 1905, and 1913 of title 18, United
14 States Code;

15 (III) sections 1343, 1344, and
16 1349(b) of title 31, United States
17 Code;

18 (IV) chapter 171 of title 28,
19 United States Code (commonly known
20 as the “Federal Tort Claims Act”)
21 and any other Federal tort liability
22 statute;

23 (V) the Ethics in Government
24 Act of 1978 (5 U.S.C. App.); and

1 (VI) chapter 21 of title 41,
2 United States Code;

3 (iii) shall not have access to any trade
4 secrets or to any other nonpublic informa-
5 tion which is of commercial value to the
6 private-sector organization from which the
7 employee is assigned;

8 (iv) may perform work that is consid-
9 ered inherently governmental in nature
10 only when requested in writing by the Sec-
11 retary; and

12 (v) may not be used to circumvent
13 any limitation or restriction on the size of
14 the workforce of the Department.

15 (H) PROHIBITION AGAINST CHARGING
16 CERTAIN COSTS TO THE FEDERAL GOVERN-
17 MENT.—A private-sector organization may not
18 charge the Department or any other agency of
19 the Federal Government, as direct or indirect
20 costs under a Federal contract, the costs of pay
21 or benefits paid by the organization to an em-
22 ployee assigned to a Department organization
23 under this subsection for the period of the as-
24 signment.

25 (I) EXPENSES.—

1 (i) IN GENERAL.—The Secretary may
2 pay for travel and other work-related ex-
3 penses associated with individuals partici-
4 pating in the pilot program established
5 under subsection (b). The Secretary shall
6 not pay for lodging or per diem expenses
7 for employees of a private sector organiza-
8 tion, unless such expenses are in further-
9 ance of work-related travel other than par-
10 ticipating in the pilot program.

11 (ii) BACKGROUND INVESTIGATION.—A
12 private person supporting an individual
13 participating in the pilot program may pay
14 for a background investigation associated
15 with the participation of the individual in
16 the pilot program.

17 (J) MAXIMUM NUMBER OF PARTICI-
18 PANTS.—Not more than 250 individuals may
19 concurrently participate in the pilot program es-
20 tablished under subsection (b).

21 (4) DETAILING OF PARTICIPANTS.—With the
22 consent of an individual participating in the pilot
23 program established under subsection (b), the Sec-
24 retary may, under the pilot program, detail the indi-
25 vidual to another Federal department or agency.

1 (5) SUNSET.—The pilot program established
2 under subsection (b) shall terminate on the date that
3 is 7 years after the date of enactment of this Act.

4 (6) REPORTS.—

5 (A) PRELIMINARY REPORT.—Not later
6 than 2 years after the date of enactment of this
7 Act, the Secretary shall submit to the congress-
8 sional homeland security committees a prelimi-
9 nary report describing the implementation of
10 the pilot program established under subsection
11 (b), including the number of participating em-
12 ployees from the Department and from private
13 sector organizations, the departmental missions
14 or programs carried out by employees partici-
15 pating in the pilot program, and recommenda-
16 tions to maximize efficiencies and the effective-
17 ness of the pilot program in order to support
18 Department cybersecurity missions and objec-
19 tives.

20 (B) FINAL REPORT.—Not later than 6
21 years after the date of enactment of this Act,
22 the Secretary shall submit to the congressional
23 homeland security committees a final report de-
24 scribing the implementation of the pilot pro-
25 gram established under subsection (b), includ-

1 ing the number of participating employees from
2 the Department and from private sector organi-
3 zations, the departmental missions or programs
4 carried out by employees participating in the
5 pilot program, and providing a recommendation
6 on whether the pilot program should be made
7 permanent.

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

12 **“SEC. 2218. CYBERSECURITY APPRENTICESHIPS.**

13 “‘The director of cybersecurity and infrastructure se-
14 curity agency may establish a cybersecurity apprenticeship
15 program in coordination with the National Institutes of
16 Standards and Technology National Initiative for Cyberse-
17 curity Education and the Department of Labor Appren-
18 ticeship Office.’”.

19 (c) CLERICAL AMENDMENT.—The table of contents
20 in section 1(b) of the Homeland Security Act of 2002 is
21 amended by inserting after the item relating to section
22 2217, as added by this title, the following new item:

 “Sec. 2218. Cybersecurity apprenticeships.”.

23 **SEC. 308. ELECTION SECURITY.**

24 (a) ELECTION INFRASTRUCTURE DESIGNATION.—
25 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

1 (E) provide physical and protective secu-
2 rity tools, training and resources; and

3 (2) employ field-base cybersecurity advisors and
4 protective security advisors.

5 **SEC. 309. PROTECTION FROM LIABILITY.**

6 Section 2224 of the Homeland Security Act (6 U.S.C.
7 673) is amending by adding at the end the following new
8 subsections:

9 “(i) MONITORING OF INFORMATION SYSTEMS.—No
10 cause of action shall lie or be maintained in any court
11 against any private entity, and such action shall be
12 promptly dismissed, for the monitoring of an information
13 system and information under section 104(a) that is con-
14 ducted in accordance with this title.

15 “(j) SHARING OR RECEIPT OF CYBER THREAT INDI-
16 CATORS.—

17 “(1) IN GENERAL.—No cause of action shall lie
18 or be maintained in any court against any private
19 entity, and such action shall be promptly dismissed,
20 for the sharing or receipt of a cyber threat indicator
21 or defensive measure under section 104(c) if—

22 “(A) such sharing or receipt is conducted
23 in accordance with this title; and

24 “(B) in a case in which a cyber threat in-
25 dicator or defensive measure is shared with the

1 Federal Government, the cyber threat indicator
2 or defensive measure is shared in a manner
3 that is consistent with section 105(c)(1)(B) and
4 the sharing or receipt, as the case may be, oc-
5 curs after the earlier of—

6 “(i) the date on which the interim
7 policies and procedures are submitted to
8 Congress under section 105(a)(1) and
9 guidelines are submitted to Congress under
10 section 105(b)(1); or

11 “(ii) the date that is 60 days after the
12 date of the enactment of this subsection.

13 “(2) RULE OF CONSTRUCTION.—Nothing in
14 this subsection may be construed to—

15 “(A) create a duty to—

16 “(i) share a cyber threat indicator or
17 defensive measure; or

18 “(ii) warn or act based on the receipt
19 of a cyber threat indicator or defensive
20 measure; or

21 “(B) undermine or limit the availability of
22 otherwise applicable common law or statutory
23 defenses.”.

1 **SEC. 310. PERMANENT EXTENSION OF CHEMICAL FACILITY**
2 **ANTI-TERRORISM STANDARDS PROGRAM OF**
3 **THE DEPARTMENT OF HOMELAND SECURITY.**

4 Section 5 of the Protecting and Securing Chemical
5 Facilities from Terrorist Attacks Act of 2014 (Public Law
6 113–254; 6 U.S.C. 621 note) is repealed.

7 **SEC. 311. CYBERSECURITY RESEARCH AND DEVELOPMENT**
8 **PROJECTS.**

9 (a) CYBERSECURITY RESEARCH AND DEVELOP-
10 MENT.—

11 (1) IN GENERAL.—Title III of the Homeland
12 Security Act of 2002 (6 U.S.C. 181 et seq.), as
13 amended by title I of this Act, is further amended
14 by adding at the end the following new section:

15 **“SEC. 322. CYBERSECURITY RESEARCH AND DEVELOP-**
16 **MENT.**

17 “(a) IN GENERAL.—The Under Secretary for Science
18 and Technology shall support the research, development,
19 testing, evaluation, and transition of cybersecurity tech-
20 nologies, including fundamental research to improve the
21 sharing of information, information security, analytics,
22 and methodologies related to cybersecurity risks and inci-
23 dents, consistent with current law.

24 “(b) ACTIVITIES.—The research and development
25 supported under subsection (a) shall serve the components
26 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-

1 vacy of information to detect and prevent cybersecu-
2 rity risks and incidents;

3 “(8) assist the development and accelerate the
4 deployment of information security measures, in ad-
5 dition to perimeter-based protections;

6 “(9) assist the development and accelerate the
7 deployment of technologies to detect improper infor-
8 mation access by authorized users;

9 “(10) assist the development and accelerate the
10 deployment of cryptographic technologies to protect
11 information at rest, in transit, and in use;

12 “(11) assist the development and accelerate the
13 deployment of methods to promote greater software
14 assurance;

15 “(12) assist the development and accelerate the
16 deployment of tools to securely and automatically
17 update software and firmware in use, with limited or
18 no necessary intervention by users and limited im-
19 pact on concurrently operating systems and proc-
20 esses; and

21 “(13) assist in identifying and addressing un-
22 identified or future cybersecurity threats.

23 “(c) COORDINATION.—In carrying out this section,
24 the Under Secretary for Science and Technology shall co-
25 ordinate 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

1 on the public or private information systems and
2 networks of information systems.

3 “(e) DEFINITIONS.—In this section:

4 “(1) CYBERSECURITY RISK.—The term ‘cyber-
5 security risk’ has the meaning given the term in sec-
6 tion 2209.

7 “(2) HOMELAND SECURITY ENTERPRISE.—The
8 term ‘homeland security enterprise’ means relevant
9 governmental and nongovernmental entities involved
10 in homeland security, including Federal, State, local,
11 and Tribal government officials, private sector rep-
12 resentatives, academics, and other policy experts.

13 “(3) INCIDENT.—The term ‘incident’ has the
14 meaning given the term in section 2209.

15 “(4) INFORMATION SYSTEM.—The term ‘infor-
16 mation system’ has the meaning given the term in
17 section 3502 of title 44, United States Code.

18 “(5) SOFTWARE ASSURANCE.—The term ‘soft-
19 ware assurance’ means confidence that software—

20 “(A) is free from vulnerabilities, either in-
21 tentiously designed into the software or acci-
22 dentally inserted at any time during the life
23 cycle of the software; and

24 “(B) functioning in the intended manner.”.

1 (2) CLERICAL AMENDMENT.—The table of con-
2 tents in section 1(b) of the Homeland Security Act
3 of 2002 is amended by inserting after the item relat-
4 ing to section 321, as added by title I of this Act,
5 the following new item:

“Sec. 322. Cybersecurity research and development.”.

6 (b) RESEARCH AND DEVELOPMENT PROJECTS.—
7 Section 831 of the Homeland Security Act of 2002 (6
8 U.S.C. 391) is amended—

9 (1) in subsection (a)—

10 (A) in the matter preceding paragraph (1),
11 by striking “2017” and inserting “2022”; and

12 (B) in paragraph (2), by striking “under
13 section 845 of the National Defense Authoriza-
14 tion Act for Fiscal Year 1994 (Public Law
15 103–160). In applying the authorities of that
16 section 845, subsection (c) of that section shall
17 apply with respect to prototype projects under
18 this paragraph, and the Secretary shall perform
19 the functions of the Secretary of Defense under
20 subsection (d) thereof” and inserting “under
21 section 2371b of title 10, United States Code,
22 and the Secretary shall perform the functions of
23 the Secretary of Defense as prescribed.”;

24 (2) in subsection (c)—

1 (A) in paragraph (1), in the matter pre-
2 ceding subparagraph (A), by striking “2017”
3 and inserting “2022”; and

4 (B) by amending paragraph (2) to read as
5 follows:

6 “(2) REPORT.—The Secretary shall annually
7 submit to the Committee on Homeland Security and
8 the Committee on Science, Space, and Technology of
9 the House of Representatives and the Committee on
10 Homeland Security and Governmental Affairs of the
11 Senate a report detailing the projects for which the
12 authority granted by subsection (a) was utilized, the
13 rationale for such utilizations, the funds spent uti-
14 lizing such authority, the extent of cost-sharing for
15 such projects among Federal and non-Federal
16 sources, the extent to which utilization of such au-
17 thority has addressed a homeland security capability
18 gap or threat to the homeland identified by the De-
19 partment, the total amount of payments, if any, that
20 were received by the Federal Government as a result
21 of the utilization of such authority during the period
22 covered by each such report, the outcome of each
23 project for which such authority was utilized, and
24 the results of any audits of such projects.”;

1 (3) in subsection (d), by striking “as defined in
2 section 845(e) of the National Defense Authorization
3 Act for Fiscal Year 1994 (Public Law 103–160; 10
4 U.S.C. 2371 note)” and inserting “as defined in sec-
5 tion 2371b(e) of title 10, United States Code.”; and

6 (4) by adding at the end the following:

7 “(e) TRAINING.—The Secretary shall develop a train-
8 ing program for acquisitions staff on the utilization of the
9 authority provided under subsection (a) to ensure account-
10 ability and effective management of projects consistent
11 with the Program Management Improvement Account-
12 ability Act (Public Law 114–264; 130 Stat. 1371) and
13 the amendments made by such Act.”.

14 (c) NO ADDITIONAL FUNDS AUTHORIZED.—No addi-
15 tional funds are authorized to carry out the requirements
16 of this section and the amendments made by this section.
17 Such requirements shall be carried out using amounts oth-
18 erwise authorized.

19 **SEC. 312. LOAN REPAYMENT PROGRAM.**

20 (a) AGREEMENT.—The Secretary of Homeland Secu-
21 rity shall enter into an agreement with each individual in
22 a cybersecurity position identified by a Federal agency
23 pursuant to section 303 of the Federal Cybersecurity
24 Workforce Assessment Act of 2015, under which—

1 (1) the individual agrees serve in such a posi-
2 tion for not less than a 5-year period; and

3 (2) for each year of such service, the Secretary
4 shall repay an amount of principal and interest, as
5 specified in the agreement, that the individual owes
6 on qualifying educational loans.

7 (b) QUALIFYING EDUCATIONAL LOAN DEFINED.—

8 The term “qualifying educational loan” means a loan
9 made under part D of title IV of the Higher Education
10 Act of 1965 (20 U.S.C. 1087a) or private education loan
11 (as defined in section 140 of the Truth in Lending Act)
12 received by an individual for the cost of attendance (as
13 defined in section 472 of the Higher Education Act of
14 1965 (20 U.S.C. 1087ll) at an institution designated by
15 the Department as a Center for Academic Excellence in
16 Cybersecurity.

17 (c) BREACH REMEDIES.—

18 (1) IN GENERAL.—Subject to paragraph (1), an
19 agreement under subsection (a) shall provide for
20 remedies in a case in which an individual does not
21 comply with the service requirement under sub-
22 section (a)(1), including repayment or partial repay-
23 ment of the loan repayment amount received under
24 subsection (a), with interest.

1 (2) WAIVER.—The Secretary of Homeland Se-
2 curity waive a remedy provided for under paragraph
3 (1) in the case of extreme hardship or extreme need,
4 as determined by the Secretary.

5 (d) ADMINISTRATION.—The Secretary of Homeland
6 Security may carry out this section directly or enter into
7 an agreement with another Federal agency or other service
8 provider to assist in the administration of this section.

9 (e) REPAYMENT SCHEDULE.—The Secretary of
10 Homeland Security may enter into an agreement with the
11 holder of any loan for which the Secretary makes pay-
12 ments under this section to establish a schedule for the
13 making of such payments.

14 (f) REGULATIONS.—Not later than 270 days after
15 the date of enactment of this subsection, the Secretary of
16 Homeland Security shall promulgate regulations to carry
17 out this section, including regulations to determine the ag-
18 gregate amount of loan repayment that an individual may
19 receive under subsection (a).

20 **SEC. 313. EXCLUSION OF CERTAIN STUDENT LOAN REPAY-**
21 **MENTS.**

22 (a) IN GENERAL.—Part III of subchapter B of chap-
23 ter 1 of the Internal Revenue Code of 1986 is amended
24 by inserting after section 139H the following new section:

1 **“SEC. 139I. CERTAIN STUDENT LOAN REPAYMENTS.**

2 “Gross income shall not include any amount of loan
3 repayment received under section 312(a) of the Keep
4 America Secure Act.”.

5 (b) CLERICAL AMENDMENT.—The table of sections
6 for part III of subchapter B of chapter 1 of such Code
7 is amended by inserting after the item relating to section
8 139H the following new item:

“Sec. 139I. Certain student loan repayments.”.

9 (c) EFFECTIVE DATE.—The amendments made by
10 this section shall apply to taxable years beginning after
11 December 31, 2019.

12 **SEC. 314. SCHOLARSHIP FOR SERVICE.**

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

17 **“SEC. 2219. SCHOLARSHIP FOR SERVICE.**

18 “(a) IN GENERAL.—The Secretary, acting through
19 the Director, may establish a scholarship program (in this
20 section referred to as the ‘program’) to recruit and train
21 information technology, cybersecurity, and industrial con-
22 trol system security professionals to work in the Agency.

23 “(b) ELEMENTS.—The program shall—

24 “(1) provide scholarships through institutions
25 of higher education, including community colleges,

1 that are designated as National Centers of Academic
2 Excellence in cybersecurity by the Department, to
3 students who are enrolled in programs of study at
4 such institutions leading to degrees or specialized
5 program certifications in the cybersecurity field;

6 “(2) provide scholarship recipients with summer
7 internship opportunities or other meaningful tem-
8 porary appointments relating to the cybersecurity
9 mission of the Department; and

10 “(3) prioritize the employment placement in the
11 Department of at least 80 percent of scholarship re-
12 cipients.

13 “(c) AMOUNT.—A scholarship awarded under the
14 program shall be in an amount that—

15 “(1) covers the recipient’s tuition and fees for
16 not more than 4 years; and

17 “(2) provides the recipient with a stipend.

18 “(d) POST-AWARD EMPLOYMENT OBLIGATIONS.—
19 Each scholarship recipient, as a condition of receiving a
20 scholarship under the program, shall enter into an agree-
21 ment under which the recipient agrees to work for a period
22 of five years in the cybersecurity mission of the Depart-
23 ment after receipt of the student’s degree or specialized
24 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

1 of post-award employment and up-to-date contact in-
2 formation.

3 “(2) TERMS.—A scholarship recipient under the
4 program shall be liable to the United States as pro-
5 vided in subsection (i) if the recipient—

6 “(A) does not maintain an acceptable level
7 of academic standing at the applicable institu-
8 tion described in subsection (b)(1), as deter-
9 mined by the Secretary, acting through the Di-
10 rector;

11 “(B) is dismissed for disciplinary reasons
12 from such applicable institution;

13 “(C) withdraws from the eligible degree
14 program before completing the program of
15 study;

16 “(D) declares an intention to not fulfill the
17 post-award employment obligation under the
18 program; or

19 “(E) does not fulfill the post-award em-
20 ployment obligation under the program.

21 “(g) AMOUNT OF REPAYMENT.—

22 “(1) LESS THAN ONE YEAR OF SERVICE.—If a
23 circumstance described in subsection (f)(2) occurs
24 before the completion of one year of a post-award
25 employment obligation under the program, the total

1 monetary amount of the scholarship award received
2 by the recipient under the program shall be—

3 “(A) repaid; or

4 “(B) treated as a loan to be repaid in ac-
5 cordance with subsection (h).

6 “(2) ONE OR MORE YEARS OF SERVICE.—If a
7 circumstance described in subparagraph (D) or (E)
8 of subsection (f)(2) occurs after the completion of
9 one or more years of a post-award employment obli-
10 gation under the program, the total monetary
11 amount of the scholarship awards received by the re-
12 cipient under the program, reduced by the ratio of
13 the number of years of service completed divided by
14 the number of years of service required, shall be—

15 “(A) repaid; or

16 “(B) treated as a loan to be repaid in ac-
17 cordance with subsection (h).

18 “(h) REPAYMENTS.—A loan described in subsection
19 (g) shall be—

20 “(1) treated as a Federal Direct Unsubsidized
21 Stafford Loan under part D of title IV of the High-
22 er Education Act of 1965 (20 U.S.C. 1087a et seq.);
23 and

24 “(2) subject to repayment, together with inter-
25 est thereon accruing from the date of the scholarship

1 award, in accordance with terms and conditions
2 specified by the Secretary, acting through the Direc-
3 tor, (in consultation with the Secretary of Edu-
4 cation) in regulations promulgated to carry out this
5 subsection.

6 “(i) COLLECTION OF REPAYMENT.—

7 “(1) IN GENERAL.—In the event that a scholar-
8 ship recipient is required to repay the scholarship
9 award under this section, an institution described in
10 subsection (b)(1) providing the scholarship shall—

11 “(A) determine the repayment amounts
12 and notify the recipient and the Secretary of
13 the amounts owed; and

14 “(B) collect the repayment amounts within
15 a period of time as determined by the Sec-
16 retary, or the repayment amounts shall be
17 treated as a loan in accordance with subsection
18 (h).

19 “(2) RETURNED TO TREASURY.—Except as
20 provided in paragraph (3), any repayment under this
21 subsection shall be returned to the Treasury of the
22 United States.

23 “(3) RETAINED PERCENTAGE.—An institution
24 described in subsection (b)(1) may retain a percent-
25 age of any repayment such institution collects under

1 (b) ELEMENTS OF REVIEW.—The review conducted
2 in accordance with subsection (a) shall include the fol-
3 lowing elements:

4 (1) An assessment of how additional budget re-
5 sources could be used by the Cybersecurity and In-
6 frastructure Security Agency for projects and pro-
7 grams that—

8 (A) support the national risk management
9 mission;

10 (B) support public and private-sector cy-
11 bersecurity;

12 (C) promote public-private integration; and

13 (D) provide situational awareness of cyber-
14 security threats.

15 (2) A force structure assessment of the Cyber-
16 security and Infrastructure Security Agency, includ-
17 ing—

18 (A) a determination of the appropriate size
19 and composition of personnel to carry out the
20 mission requirements of the Agency, as well as
21 the recommendations detailed in the U.S.
22 Cyberspace Solarium Commission’s Report re-
23 garding the Agency;

24 (B) as assessment of whether existing per-
25 sonnel 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,

1 and recommendations regarding future facility
2 requirements.

3 (c) SUBMISSION OF REVIEW.—Not later than one
4 year after the date of the enactment of this Act, the Sec-
5 retary of Homeland Security shall submit to the Com-
6 mittee on Homeland Security of the House of Representa-
7 tives and the Committee on Homeland Security and Gov-
8 ernmental Affairs of the Senate a report detailing the re-
9 sult of the review conducted in accordance with subsection
10 (a), including recommendations to address any identified
11 gaps.

12 (d) GENERAL SERVICES ADMINISTRATION RE-
13 VIEW.—

14 (1) SUBMISSION OF ASSESSMENT.—Upon sub-
15 mission to the Committee on Homeland Security of
16 the House of Representatives and the Committee on
17 Homeland Security and Governmental Affairs of the
18 Senate of the report required under subsection (c),
19 the Director of the Cybersecurity and Infrastructure
20 Security Agency of the Department of Homeland Se-
21 curity shall submit to the Administrator of the Gen-
22 eral Services Administration the results of the as-
23 sessment required under subsection (b)(2)(E).

24 (2) REVIEW.—The Administrator of the Gen-
25 eral Services Administration shall—

1 (A) conduct a review of Cybersecurity and
2 Infrastructure Security Agency assessment re-
3 quired under subsection (b)(2)(E); and

4 (B) make recommendations regarding re-
5 sources needed to procure or build a new facil-
6 ity or augment existing facilities to ensure suffi-
7 cient size and accommodations to fully support
8 current and projected mission requirements, in-
9 cluding the integration of personnel from the
10 private sector and other Federal departments
11 and agencies.

12 (3) SUBMISSION OF REVIEW.—Not later than
13 30 days after receipt of the assessment in accord-
14 ance with paragraph (1), the Administrator of the
15 General Services Administration shall submit to the
16 President, the Secretary of Homeland Security, the
17 Committee on Homeland Security and Governmental
18 Affairs of the Senate, and the Committee on Home-
19 land Security of the House of Representatives the
20 review required under paragraph (2).

21 **SEC. 316. STRATEGY TO SECURE EMAIL.**

22 (a) IN GENERAL.—Not later than December 31,
23 2021, the Secretary of Homeland Security shall develop
24 and submit to Congress a strategy, including rec-
25 ommendations, 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

1 recommendations for defraying such costs, if appli-
2 cable.

3 (c) CONSULTATION.—In developing the strategies
4 and recommendations under subsection (a), the Secretary
5 of Homeland Security may, as appropriate, consult with
6 representatives from the information technology sector.

7 (d) EXEMPTION.—The Federal Advisory Committee
8 Act (5 U.S.C. App.) shall not apply to this section or to
9 any action to implement this section.

10 (e) DEFINITION.—In this section, the term “Domain-
11 based Message Authentication, Reporting, and Conform-
12 ance” means an email authentication, policy, and report-
13 ing protocol that verifies the authenticity of the sender of
14 an email and blocks and reports to the sender fraudulent
15 accounts.

16 **SEC. 317. STRENGTHENING FEDERAL NETWORKS.**

17 (a) AUTHORITY.—Section 3553(b) of title 44, United
18 States Code, is amended—

19 (1) in paragraph (6)(D), by striking “; and” at
20 the end and inserting a semicolon;

21 (2) by redesignating paragraph (7) as para-
22 graph (8); and

23 (3) by inserting after paragraph (6) the fol-
24 lowing new paragraph:

1 “(7) hunting for and identifying, with or with-
2 out advance notice, threats and vulnerabilities within
3 Federal information systems; and”.

4 (b) **BINDING OPERATIONAL DIRECTIVE.**—Not later
5 than 1 year after the date of the enactment of this section,
6 the Secretary of Homeland Security shall issue a binding
7 operational directive pursuant to subsection (b)(2) of sec-
8 tion 3553 of title 44, United States Code, to implement
9 paragraph (7) of section 3553(b) of title 44, United States
10 Code, as added by subsection (a).

11 **SEC. 318. AUTHORIZATION OF APPROPRIATIONS.**

12 For necessary expenses of the Cybersecurity and In-
13 frastructure Security Agency of the Department of Home-
14 land Security, including to carry out this title and the
15 amendments made by this title, there is authorized to be
16 appropriated to the Agency the following:

17 (1) \$2,400,000,000 for fiscal year 2021.

18 (2) \$2,800,000,000 for fiscal year 2022.

19 **TITLE IV—BORDER AND VISA**
20 **SECURITY**

21 **SEC. 401. ADDITIONAL U.S. CUSTOMS AND BORDER PRO-**
22 **TECTION AGENTS AND OFFICERS.**

23 (a) **U.S. BORDER PATROL AGENTS AND PROCESSING**
24 **COORDINATORS.**—Not later than September 30, 2024, the
25 Commissioner of U.S. Customs and Border Protection

1 shall hire, train, and assign sufficient U.S. Border Patrol
2 personnel to maintain an active duty presence of not fewer
3 than 26,370 full-time equivalent agents and not fewer
4 than 1,200 processing coordinators.

5 (b) CBP OFFICERS.—Not later than September 30,
6 2024, the Commissioner of U.S. Customs and Border Pro-
7 tection shall hire, train, and assign sufficient U.S. Cus-
8 toms and Border Protection officers to maintain an active
9 duty presence of not fewer than 27,725 full-time equiva-
10 lent officers.

11 (c) AIR AND MARINE OPERATIONS.—Not later than
12 September 30, 2024, the Commissioner of U.S. Customs
13 and Border Protection shall hire, train, and assign suffi-
14 cient agents for Air and Marine Operations of U.S. Cus-
15 toms and Border Protection to maintain not fewer than
16 1,675 full-time equivalent agents and not fewer than 264
17 Marine and Air Interdiction Agents for southern border
18 air and maritime operations.

19 (d) PROFESSIONAL SUPPORT STAFF.—Not later
20 than September 30, 2024, the Secretary of Homeland Se-
21 curity shall hire, train, and assign sufficient professional
22 support staff for the recruitment, hiring, training, and
23 maintenance of the personnel authorized under sub-
24 sections (a) through (c).

1 (e) GAO REPORT.—If the staffing levels required
2 under this section are not achieved by September 30,
3 2024, the Comptroller General of the United States shall
4 conduct a review of the reasons why such levels were not
5 achieved.

6 (f) AUTHORIZATION OF APPROPRIATIONS.—There is
7 authorized to be appropriated \$1,250,000,000 for each of
8 fiscal years 2021 through 2024 to carry out subsection
9 (a) through (d).

10 **SEC. 402. ESTABLISHMENT OF WORKLOAD STAFFING MOD-**
11 **ELS FOR U.S. BORDER PATROL AND AIR AND**
12 **MARINE OPERATIONS OF CBP.**

13 (a) IN GENERAL.—Not later than one year after the
14 date of the enactment of this Act, the Commissioner of
15 U.S. Customs and Border Protection, in coordination with
16 the Under Secretary for Management, the Chief Human
17 Capital Officer, and the Chief Financial Officer of the De-
18 partment of Homeland Security, shall implement a work-
19 load staffing model for each of the following:

20 (1) The U.S. Border Patrol.

21 (2) Air and Marine Operations of U.S. Customs
22 and Border Protection.

23 (b) RESPONSIBILITIES OF THE COMMISSIONER OF
24 CBP.—Subsection (c) of section 411 of the Homeland Se-
25 curity Act of 2002 (6 U.S.C. 211), is amended—

1 (1) by redesignating paragraphs (18) and (19)
2 as paragraphs (20) and (21), respectively; and

3 (2) by inserting after paragraph (17) the fol-
4 lowing new paragraphs:

5 “(18) implement a staffing model that includes
6 consideration for essential frontline operator activi-
7 ties and functions, variations in operating environ-
8 ments, present and planned infrastructure, present
9 and planned technology, and required operations
10 support levels for the U.S. Border Patrol, Air and
11 Marine Operations, and the Office of Field Oper-
12 ations, to manage and assign personnel of such enti-
13 ties to ensure field and support posts possess ade-
14 quate resources to carry out duties specified in this
15 section;

16 “(19) develop standard operating procedures
17 for a workforce tracking system within the U.S.
18 Border Patrol, Air and Marine Operations, and the
19 Office of Field Operations, train the workforce of
20 each of such entities on the use, capabilities, and
21 purpose of such system, and implement internal con-
22 trols to ensure timely and accurate scheduling and
23 reporting of actual completed work hours and activi-
24 ties;”.

1 (c) REPORT.—Not later than one year after the date
2 of the enactment of this Act with respect to subsection
3 (a) and paragraphs (18) and (19) of section 411(c) of the
4 Homeland Security Act of 2002 (as amended by sub-
5 section (b)), and annually thereafter with respect to such
6 paragraphs (18) and (19), the Secretary of Homeland Se-
7 curity shall submit to the Committee on Homeland Secu-
8 rity of the House of Representatives and the Committee
9 on Homeland Security and Governmental Affairs of the
10 Senate a status update on the implementation of such sub-
11 section (a) and such paragraphs (18) and (19), and status
12 updates on such paragraphs (18) and (19), as well as all
13 relevant workload staffing models. Such status updates
14 shall include information on data sources and methodology
15 used to generate such staffing models.

16 (d) INSPECTOR GENERAL REVIEW.—Not later than
17 120 days after the Commissioner of U.S. Customs and
18 Border Protection develops a workload staffing model pur-
19 suant to subsection (a), the Inspector General of the De-
20 partment of Homeland Security shall review such model
21 and provide feedback to the Secretary of Homeland Secu-
22 rity and the Committee on Homeland Security of the
23 House of Representatives and the Committee on Home-
24 land Security and Governmental Affairs of the Senate re-
25 garding the degree to which such model is responsive to

1 Inspector General recommendations, including rec-
2 ommendations from the Inspector General’s February
3 2019 audit, and as appropriate, any further recommenda-
4 tions to improve such model.

5 **SEC. 403. U.S. CUSTOMS AND BORDER PROTECTION RETEN-**
6 **TION INCENTIVES.**

7 (a) IN GENERAL.—Chapter 97 of title 5, United
8 States Code, is amended by adding at the end the fol-
9 lowing:

10 **“§ 9702. U.S. Customs and Border Protection tem-**
11 **porary employment authorities**

12 “(a) DEFINITIONS.—In this section—

13 “(1) the term ‘CBP employee’ means an em-
14 ployee of U.S. Customs and Border Protection;

15 “(2) the term ‘Commissioner’ means the Com-
16 missioner of U.S. Customs and Border Protection;

17 “(3) the term ‘Director’ means the Director of
18 the Office of Personnel Management;

19 “(4) the term ‘Secretary’ means the Secretary
20 of Homeland Security; and

21 “(5) the term ‘appropriate congressional com-
22 mittees’ means the Committee on Oversight and Re-
23 form, the Committee on Homeland Security, and the
24 Committee on Ways and Means of the House of
25 Representatives, and the Committee on Homeland

1 Security and Governmental Affairs and the Com-
2 mittee on Finance of the Senate.

3 “(b) DIRECT HIRE AUTHORITY; RECRUITMENT AND
4 RELOCATION BONUSSES; RETENTION BONUSSES.—

5 “(1) DIRECT HIRE AUTHORITY.—The Secretary
6 may appoint, without regard to sections 3309
7 through 3319, candidates to positions in the com-
8 petitive service within U.S. Customs and Border
9 Protection if the Secretary has given public notice of
10 such positions before making any such appointment.

11 “(2) RECRUITMENT AND RELOCATION BO-
12 NUSSES.—The Secretary may pay a recruitment or
13 relocation bonus of up to 50 percent of the annual
14 rate of basic pay to an individual CBP employee as
15 of the first day of the applicable service period (as
16 prescribed by a written service agreement described
17 in subparagraph (B)) multiplied by the number of
18 years (including a fractional part of a year) in the
19 service period if—

20 “(A) the Secretary determines that condi-
21 tions consistent with the conditions described in
22 paragraphs (1) and (2) of subsection (b) of sec-
23 tion 5753 are satisfied with respect to the indi-
24 vidual (without regard to the regulations ref-
25 erenced 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—

1 “(I) the commencement and ter-
2 mination dates of the required service
3 period (or provisions for the deter-
4 mination thereof);

5 “(II) the amount of the bonus;
6 and

7 “(III) other terms and conditions
8 under which the bonus is payable,
9 subject to the requirements of this
10 subsection, including—

11 “(aa) the conditions under
12 which the agreement may be ter-
13 minated before the agreed-upon
14 service period has been com-
15 pleted; and

16 “(bb) the effect of a termi-
17 nation described in item (aa).

18 “(4) RULES FOR BONUSES.—

19 “(A) MAXIMUM BONUS LIMITATIONS.—

20 “(i) UNDER PARAGRAPH (2).—A CBP
21 employee may not receive a total amount
22 of bonuses under paragraph (2) in excess
23 of 100 percent of the annual rate of basic
24 pay of the employee as of the first day of
25 the applicable service period.

1 “(ii) UNDER PARAGRAPH (3).—A
2 bonus paid to any CBP employee under
3 paragraph (3) may not exceed 50 percent
4 of the annual rate of basic pay of the em-
5 ployee.

6 “(B) RELATIONSHIP TO BASIC PAY.—A
7 bonus paid under paragraph (2) or (3) shall not
8 be considered part of the basic pay of the CBP
9 employee for any purpose, including for retire-
10 ment or in computing a lump-sum payment to
11 the covered employee for accumulated and ac-
12 crued annual leave under section 5551 or sec-
13 tion 5552.

14 “(C) PERIOD OF SERVICE FOR RECRUIT-
15 MENT, RELOCATION, AND RETENTION BO-
16 NUSES.—

17 “(i) RESTRICTION.—A bonus paid
18 under paragraph (3) may not be based on
19 any period of such service which is the
20 basis for a recruitment or relocation bonus
21 under paragraph (2).

22 “(ii) FURTHER RESTRICTION.—A
23 bonus paid under paragraph (2) or (3)
24 may not be based on any period of service
25 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

1 each report, the Secretary shall provide such infor-
2 mation as the Director determines is appropriate to
3 ensure appropriate use of authorities under such
4 subsections. Each report shall also include an assess-
5 ment of—

6 “(A) the impact of the use of authorities
7 under subsections (b) and (c) on implementa-
8 tion of meeting staffing levels as described in
9 section 401;

10 “(B) whether the authorities solved hiring
11 and retention challenges at the agency, includ-
12 ing at specific locations;

13 “(C) whether hiring and retention chal-
14 lenges still exist at the agency or specific loca-
15 tions; and

16 “(D) whether the Secretary needs to con-
17 tinue to use authorities provided under this sec-
18 tion at the agency or at specific locations.

19 “(2) CONSIDERATION.—In compiling a report
20 under paragraph (1), the Secretary shall consider—

21 “(A) whether any CBP employee accepted
22 an employment incentive under subsection (b)
23 and (c) and then transferred to a new location
24 or left U.S. Customs and Border Protection;
25 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-

1 sources flexibilities for employees who are in-
2 volved in the recruitment, hiring, assessment, or
3 selection of candidates, as well as the retention
4 of current employees.

5 “(B) Regular training sessions for per-
6 sonnel who are critical to filling open positions
7 in rural or remote areas.

8 “(C) The development of pilot programs or
9 other programs, as appropriate, consistent with
10 authorities provided to the Secretary to address
11 identified hiring challenges, including in rural
12 or remote areas.

13 “(D) Developing and enhancing strategic
14 recruiting efforts through the relationships with
15 institutions of higher education, as defined in
16 section 102 of the Higher Education Act of
17 1965 (20 U.S.C. 1002), veterans transition and
18 employment centers, and job placement pro-
19 gram in regions that could assist in filling posi-
20 tions in rural or remote areas.

21 “(E) Examination of existing agency pro-
22 grams on how to most effectively aid spouses
23 and families of individuals who are candidates
24 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

1 such paragraph has improved the hiring
2 and retention ability of the Secretary; and

3 “(ii) make any appropriate updates to
4 the strategy under such paragraph.

5 “(B) INFORMATION.—The evaluation con-
6 ducted under subparagraph (A) shall include
7 the following:

8 “(i) Any reduction in the time taken
9 by the Secretary to fill mission-critical po-
10 sitions, including in rural or remote areas.

11 “(ii) A general assessment of the im-
12 pact of the strategy implemented under
13 paragraph (1) on hiring challenges, includ-
14 ing in rural or remote areas.

15 “(iii) Other information the Secretary
16 determines relevant.

17 “(g) INSPECTOR GENERAL REVIEW.—Not later than
18 two years after the date of the enactment of this section,
19 the Inspector General of the Department of Homeland Se-
20 curity shall review the use of hiring and pay flexibilities
21 under subsections (b) and (c) to determine whether the
22 use of such flexibilities is helping the Secretary meet hir-
23 ing and retention needs, including in rural and remote
24 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-

1 fore such date may continue until such bonus has been
2 paid, subject to the conditions specified in this section.”.

3 (b) TECHNICAL AND CONFORMING AMENDMENT.—

4 The table of sections for chapter 97 of title 5, United
5 States Code, is amended by adding at the end the fol-
6 lowing new item:

“9702. U.S. Customs and Border Protection temporary employment authori-
ties.”.

7 **SEC. 404. STUDY ON EFFICACY OF CERTAIN PERSONNEL**
8 **SCREENING METHODS FOR U.S. CUSTOMS**
9 **AND BORDER PROTECTION USE.**

10 (a) IN GENERAL.—Not later than 60 days after the
11 date of the enactment of this Act, the Secretary of Home-
12 land Security shall enter into an agreement with the Na-
13 tional Academy of Sciences to conduct a study on the effi-
14 cacy of certain personnel screening methods for U.S. Cus-
15 toms and Border Protection use. Such study shall include
16 the following:

17 (1) A review of the appropriateness of the use
18 of polygraph examinations in determining candidate
19 suitability during the U.S. Customs and Border Pro-
20 tection hiring process.

21 (2) A cost-benefit analysis of using polygraph
22 examinations for candidate suitability during the
23 U.S. Customs and Border Protection hiring process.

1 (3) A review of research related to alternatives
2 to polygraph examinations appropriate for use dur-
3 ing the U.S. Customs and Border Protection hiring
4 process.

5 (b) MATTERS INCLUDED.—The study required under
6 subsection (a) shall—

7 (1) assess prior scientific, academic, and gov-
8 ernment literature on the topics described in such
9 subsection;

10 (2) identify and examine assumptions about
11 polygraph examinations that underlie the polygraph
12 mandate under the Anti-Border Corruption Act of
13 2010 (Public Law 111–376); and

14 (3) provide specific recommendations related
15 to—

16 (A) the future use of such polygraph ex-
17 aminations, including a consideration of wheth-
18 er such polygraph mandate aligns with current
19 scientific evidence and offers a reliable indica-
20 tion of future susceptibility to corruption; and

21 (B) the appropriate alternative mecha-
22 nisms or technology, including private sector
23 tools, that could be used during the U.S. Cus-
24 toms and Border Protection hiring process to
25 pre-screen for susceptibility to corruption; and

1 (4) provide any other recommendations the Sec-
2 retary of Homeland Secretary determines relevant.

3 (c) SUBMISSION.—Not later than one year after the
4 date of the enactment of this Act, the Secretary of the
5 Homeland Security shall submit to the appropriate con-
6 gressional committees the study required under subsection
7 (a).

8 (d) DEFINITIONS.—In this section:

9 (1) APPROPRIATE CONGRESSIONAL COMMIT-
10 TEES.—The term “appropriate congressional com-
11 mittees” means the Committee on Homeland Secu-
12 rity of the House of Representatives and the Com-
13 mittee on Homeland Security and Governmental Af-
14 fairs of the Senate.

15 (2) POLYGRAPH EXAMINATIONS.—The term
16 “polygraph examinations” means polygraph exami-
17 nations conducted in accordance with section 3(1) of
18 the Anti-Border Corruption Act of 2010.

19 **SEC. 405. HIRING FLEXIBILITY.**

20 Section 3 of the Anti-Border Corruption Act of 2010
21 (Public Law 111–376; 6 U.S.C. 221) is amended by strik-
22 ing subsection (b) and inserting the following new sub-
23 sections:

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

1 by the Secretary of Homeland Security, in consultation
2 with the Director of National Intelligence.

3 “(d) **TERMINATION OF WAIVER AUTHORITY.**—The
4 authority to issue a waiver under subsection (b) shall ter-
5minate on the date that is five years after the date of the
6 enactment of the Anti-Border Corruption Reauthorization
7 Act of 2019.”.

8 **SEC. 406. SUPPLEMENTAL COMMISSIONER AUTHORITY AND**
9 **DEFINITIONS.**

10 (a) **SUPPLEMENTAL COMMISSIONER AUTHORITY.**—
11 Section 4 of the Anti-Border Corruption Act of 2010
12 (Public Law 111–376) is amended to read as follows:

13 **“SEC. 4. SUPPLEMENTAL COMMISSIONER AUTHORITY.**

14 “(a) **NON-EXEMPTION.**—An individual who receives
15 a waiver under subsection (b) of section 3 shall not be
16 exempt from other hiring requirements relating to suit-
17 ability for employment and eligibility to hold a national
18 security designated position, as determined by the Com-
19 missioner of U.S. Customs and Border Protection.

20 “(b) **BACKGROUND INVESTIGATIONS.**—Any indi-
21 vidual who receives a waiver under subsection (b) of sec-
22 tion 3 who holds a current background investigation may
23 be subject to further background investigation to the level
24 required for service as a law enforcement officer with U.S.
25 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

1 Senate information on the number, disaggregated with re-
2 spect to each of paragraphs (1), (2), and (3) of subsection
3 (b) of section 3, of waivers requested, granted, and denied,
4 and the reasons for any such denial, and the final outcome
5 of the application for employment at issue. Such informa-
6 tion shall also include the number of instances a polygraph
7 examination was administered under the conditions de-
8 scribed in subsection (d) of section 4, the result of such
9 examination, and the final outcome of the application for
10 employment at issue.”.

11 (c) DEFINITIONS.—The Anti-Border Corruption Act
12 of 2010, as amended by subsection (b) of this section, is
13 further amended by adding at the end the following new
14 section:

15 **“SEC. 6. DEFINITIONS.**

16 “In this Act:

17 “(1) LAW ENFORCEMENT OFFICER.—The term
18 ‘law enforcement officer’ has the meaning given such
19 term in sections 8331(20) and 8401(17) of title 5,
20 United States Code.

21 “(2) VETERAN.—The term ‘veteran’ has the
22 meaning given such term in section 101(2) of title
23 38, United States Code.

1 “(3) SERIOUS MILITARY OR CIVIL OFFENSE.—

2 The term ‘serious military or civil offense’ means an
3 offense for which—

4 “(A) a member of the Armed Forces may
5 be discharged or separated from service in the
6 Armed Forces; and

7 “(B) a punitive discharge is, or would be,
8 authorized for the same or a closely related of-
9 fense under the Manual for Court-Martial, as
10 pursuant to Army Regulation 635–200 chapter
11 14–12.”.

12 **SEC. 407. TECHNICAL AND CONFORMING AMENDMENT.**

13 Paragraph (15) of section 411(c) of the Homeland
14 Security Act of 2002 (6 U.S.C. 211(c)) is amended by
15 striking “section 3(1)” and inserting “section 3”.

16 **SEC. 408. PORTS OF ENTRY INFRASTRUCTURE.**

17 (a) ADDITIONAL PORTS OF ENTRY.—

18 (1) AUTHORITY.—The Administrator of Gen-
19 eral Services may, subject to section 3307 of title
20 40, United States Code, construct new ports of entry
21 along the northern border and southern border at lo-
22 cations determined by the Secretary of Homeland
23 Security.

24 (2) CONSULTATION.—

1 (A) REQUIREMENT TO CONSULT.—The
2 Secretary of Homeland Security and the Ad-
3 ministrator of General Services shall consult
4 with the Secretary of State, the Secretary of
5 the Interior, the Secretary of Agriculture, the
6 Secretary of Transportation, and appropriate
7 representatives of State and local governments,
8 Tribes, and property owners in the United
9 States prior to determining a location for any
10 new port of entry constructed pursuant to para-
11 graph (1).

12 (B) CONSIDERATIONS.—The purpose of
13 the consultations required by subparagraph (A)
14 shall be to minimize any negative impacts of
15 constructing a new port of entry on the environ-
16 ment, culture, commerce, and quality of life of
17 the communities and residents located near
18 such new port.

19 (b) EXPANSION AND MODERNIZATION OF HIGH-PRI-
20 ORITY SOUTHERN BORDER PORTS OF ENTRY.—Not later
21 than September 30, 2025, the Administrator of General
22 Services, subject to section 3307 of title 40, United States
23 Code, and in coordination with the Secretary of Homeland
24 Security, shall expand or modernize high-priority ports of
25 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

1 of such new port of entry, a description of the need
2 for such new port of entry and associated antici-
3 pated benefits, a description of the consultations un-
4 dertaken by the Secretary and the Administrator
5 pursuant to paragraph (2) of such subsection, any
6 actions that will be taken to minimize negative im-
7 pacts of such new port of entry, and the anticipated
8 time-line for construction and completion of such
9 new port of entry.

10 (2) RELATING TO EXPANSION AND MODERNIZA-
11 TION OF PORTS OF ENTRY.—Not later than 180
12 days after enactment of this Act, the Secretary of
13 Homeland Security and the Administrator of Gen-
14 eral Services shall jointly notify the Committee on
15 Homeland Security and Governmental Affairs, the
16 Committee on Finance, the Committee on Com-
17 merce, Science, and Transportation, and the Com-
18 mittee on the Judiciary of the Senate, and the Com-
19 mittee on Homeland Security, the Committee on
20 Ways and Means, the Committee on Transportation
21 and Infrastructure, and the Committee on the Judi-
22 ciary of the House of Representatives of the ports
23 of entry on the southern border that are the subject
24 of expansion or modernization pursuant to sub-
25 section (b) and the Secretary's and Administrator's

1 plan for expanding or modernizing each such port of
2 entry.

3 (e) SAVINGS PROVISION.—Nothing in this section
4 may be construed to—

5 (1) create or negate any right of action for a
6 State, local government, or other person or entity af-
7 fected by this section;

8 (2) delay the transfer of the possession of prop-
9 erty to the United States or affect the validity of
10 any property acquisitions by purchase or eminent
11 domain, or to otherwise affect the eminent domain
12 laws of the United States or of any State; or

13 (3) create any right or liability for any party.

14 (f) RULE OF CONSTRUCTION.—Nothing in this sec-
15 tion may be construed as providing the Secretary of
16 Homeland Security new authority related to the construc-
17 tion, acquisition, or renovation of real property.

18 **SEC. 409. U.S. CUSTOMS AND BORDER PROTECTION TECH-**
19 **NOLOGY UPGRADES.**

20 (a) SECURE COMMUNICATIONS.—The Commissioner
21 of U.S. Customs and Border Protection shall ensure that
22 each U.S. Customs and Border Protection officer or agent,
23 if appropriate, is equipped with a secure radio or other
24 two-way communication device, supported by system inter-

1 operability, that allows each such officer to commu-
2 nicate—

3 (1) between ports of entry and inspection sta-
4 tions; and

5 (2) with other Federal, State, Tribal, and local
6 law enforcement entities.

7 (b) BORDER SECURITY DEPLOYMENT PROGRAM.—

8 (1) EXPANSION.—Not later than September 30,
9 2023, the Commissioner of U.S. Customs and Bor-
10 der Protection shall fully implement the Border Se-
11 curity Deployment Program of U.S. Customs and
12 Border Protection and expand the integrated surveil-
13 lance and intrusion detection system at land ports of
14 entry along the southern border and the northern
15 border.

16 (2) AUTHORIZATION OF APPROPRIATIONS.—In
17 addition to amounts otherwise authorized to be ap-
18 propriated for such purpose, there is authorized to
19 be appropriated \$33,000,000 for fiscal years 2021
20 and 2022 to carry out paragraph (1).

21 (c) UPGRADE OF LICENSE PLATE READERS AT
22 PORTS OF ENTRY.—

23 (1) UPGRADE.—Not later than two years after
24 the date of the enactment of this Act, the Commis-
25 sioner of U.S. Customs and Border Protection shall

1 upgrade all existing license plate readers in need of
2 upgrade, as determined by the Commissioner, on the
3 northern and southern borders on incoming and out-
4 going vehicle lanes.

5 (2) AUTHORIZATION OF APPROPRIATIONS.—In
6 addition to amounts otherwise authorized to be ap-
7 propriated for such purpose, there is authorized to
8 be appropriated \$125,000,000 for fiscal years 2021
9 through 2022 to carry out paragraph (1).

10 (d) BIOMETRIC ENTRY-EXIT.—

11 (1) IN GENERAL.—Subtitle B of title IV of the
12 Homeland Security Act of 2002 (6 U.S.C. 211 et
13 seq.) is amended by adding at the end the following
14 new section:

15 **“SEC. 420. BIOMETRIC ENTRY-EXIT.**

16 **“(a) ESTABLISHMENT.—**The Secretary shall—

17 **“(1)** not later than 180 days after the date of
18 the enactment of this section, submit to the Com-
19 mittee on Homeland Security and the Committee on
20 the Judiciary of the House of Representatives and
21 the Committee on Homeland Security and Govern-
22 mental Affairs and the Committee on the Judiciary
23 of the Senate an implementation plan to establish a
24 biometric exit data system to complete the inte-
25 grated biometric entry and exit data system required

1 under section 7208 of the Intelligence Reform and
2 Terrorism Prevention Act of 2004 (8 U.S.C. 1365b),
3 including—

4 “(A) an integrated master schedule and
5 cost estimate, including requirements and de-
6 sign, development, operational, and mainte-
7 nance costs of such a system, that takes into
8 account prior reports on such matters issued by
9 the Government Accountability Office and the
10 Department;

11 “(B) cost-effective staffing and personnel
12 requirements of such a system that leverages
13 existing resources of the Department that takes
14 into account prior reports on such matters
15 issued by the Government Accountability Office
16 and the Department;

17 “(C) a consideration of training programs
18 necessary to establish such a system that takes
19 into account prior reports on such matters
20 issued by the Government Accountability Office
21 and the Department;

22 “(D) a consideration of how such a system
23 will affect arrival and departure wait times that
24 takes into account prior reports on such matter

1 issued by the Government Accountability Office
2 and the Department;

3 “(E) a consideration of audit capability for
4 systems procured in partnership with the pri-
5 vate sector to achieve biometric exit;

6 “(F) information received after consulta-
7 tion with private sector stakeholders, including
8 the—

9 “(i) trucking industry;

10 “(ii) airport industry;

11 “(iii) airline industry;

12 “(iv) seaport industry;

13 “(v) travel industry; and

14 “(vi) biometric technology industry;

15 “(G) a consideration of how trusted trav-
16 eler programs in existence as of the date of the
17 enactment of this section may be impacted by,
18 or incorporated into, such a system;

19 “(H) defined metrics of success and mile-
20 stones;

21 “(I) identified risks and mitigation strate-
22 gies to address such risks;

23 “(J) a consideration of how other countries
24 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 pedestrian 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 “(1) match biometric information for an indi-
2 vidual, regardless of nationality, citizenship, or im-
3 migration status, who is departing the United States
4 against biometric data previously provided to the
5 United States Government by such individual for the
6 purposes of international travel;

7 “(2) leverage the infrastructure and databases
8 of the current biometric entry and exit system estab-
9 lished pursuant to section 7208 of the Intelligence
10 Reform and Terrorism Prevention Act of 2004 (8
11 U.S.C. 1365b) for the purpose described in para-
12 graph (1); and

13 “(3) be interoperable with, and allow matching
14 against, other Federal databases that—

15 “(A) store biometrics of known or sus-
16 pected terrorists; and

17 “(B) identify visa holders who violate the
18 terms of their visas.

19 “(f) SCOPE.—

20 “(1) IN GENERAL.—The biometric exit data
21 system established under this section shall include a
22 requirement for the collection of biometric exit data
23 at the time of departure for all categories of individ-
24 uals who are required by the Secretary to provide bi-
25 ometric entry data.

1 “(2) EXCEPTION FOR CERTAIN OTHER INDIVID-
2 UALS.—This section shall not apply in the case of an
3 individual who exits and then enters the United
4 States on a passenger vessel (as such term is defined
5 in section 2101 of title 46, United States Code) the
6 itinerary of which originates and terminates in the
7 United States.

8 “(3) EXCEPTION FOR LAND PORTS OF
9 ENTRY.—This section shall not apply in the case of
10 a United States or Canadian citizen who exits the
11 United States through a land port of entry.

12 “(g) COLLECTION OF DATA.—The Secretary may not
13 require any non-Federal person to collect biometric data,
14 or contribute to the costs of collecting or administering
15 the biometric exit data system established under this sec-
16 tion, except through a mutual agreement.

17 “(h) MULTI-MODAL COLLECTION.—In carrying out
18 subsections (a)(1) and (b), the Secretary shall make every
19 effort to collect biometric data using multiple modes of
20 biometrics.

21 “(i) FACILITIES.—All facilities at which the biometric
22 exit data system established under this section is imple-
23 mented shall provide and maintain space for Federal use
24 that is adequate to support biometric data collection and
25 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:

1 “(B) PHYSICAL BARRIERS AND TACTICAL
2 INFRASTRUCTURE.—

3 “(i) IN GENERAL.—Not later than
4 September 30, 2023, the Secretary of
5 Homeland Security, in carrying out this
6 section, shall deploy along the United
7 States border the most practical and effec-
8 tive physical barriers and tactical infra-
9 structure available for achieving situational
10 awareness and operational control of the
11 border.

12 “(ii) CONSIDERATION FOR CERTAIN
13 PHYSICAL BARRIERS AND TACTICAL INFRA-
14 STRUCTURE.—The deployment of physical
15 barriers and tactical infrastructure under
16 this subparagraph shall not apply in any
17 area or region along the border where nat-
18 ural terrain features, natural barriers, or
19 the remoteness of such area or region
20 would make any such deployment ineffec-
21 tive, as determined by the Secretary, for
22 the purposes of achieving situational
23 awareness or operational control of such
24 area or region.”;

25 (iii) in subparagraph (C)—

1 (I) by amending clause (i) to
2 read as follows:

3 “(i) IN GENERAL.—In carrying out
4 this section, the Secretary of Homeland
5 Security shall consult with the Secretary of
6 the Interior, the Secretary of Agriculture,
7 appropriate representatives of Federal,
8 State, local, and tribal governments, and
9 appropriate private property owners in the
10 United States to minimize the impact on
11 the environment, culture, commerce, and
12 quality of life for the communities and
13 residents located near the sites at which
14 such physical barriers are to be con-
15 structed.”;

16 (II) in clause (ii)—

17 (aa) in subclause (I), by
18 striking “or” after the semicolon
19 at the end;

20 (bb) by amending subclause
21 (II) to read as follows:

22 “(II) delay the transfer of the
23 possession of property to the United
24 States or affect the validity of any
25 property acquisition by purchase or

1 eminent domain, or to otherwise affect
2 the eminent domain laws of the
3 United States or of any State; or”;
4 and

5 (cc) by adding at the end
6 the following new subclause:

7 “(III) create any right or liability
8 for any party.”; and

9 (iv) by striking subparagraph (D);
10 (C) in paragraph (2)—

11 (i) by striking “Attorney General”
12 and inserting “Secretary of Homeland Se-
13 curity”;

14 (ii) by striking “this subsection” and
15 inserting “this section”; and

16 (iii) by striking “construction of
17 fences” and inserting “the construction of
18 physical barriers”;

19 (D) by amending paragraph (3) to read as
20 follows:

21 “(3) AGENT SAFETY.—In carrying out this sec-
22 tion, the Secretary of Homeland Security, when de-
23 signing, constructing, and deploying physical bar-
24 riers, tactical infrastructure, or technology, shall in-
25 corporate 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

1 effective upon publication in the Federal Register.”;

2 and

3 (4) by adding after subsection (d) the following
4 new subsections:

5 “(e) TECHNOLOGY.—Not later than September 30,
6 2023, the Secretary of Homeland Security, in carrying out
7 this section, shall deploy along the United States border
8 the most practical and effective technology available for
9 achieving situational awareness and operational control of
10 the border.

11 “(f) DEFINITIONS.—In this section:

12 “(1) OPERATIONAL CONTROL.—The term ‘oper-
13 ational control’ has the meaning given such term in
14 section 2(b) of the Secure Fence Act of 2006 (8
15 U.S.C. 1701 note; Public Law 109–367).

16 “(2) PHYSICAL BARRIERS.—The term ‘physical
17 barriers’ includes reinforced fencing, border wall sys-
18 tem, and levee walls.

19 “(3) SITUATIONAL AWARENESS.—The term ‘sit-
20 uational awareness’ has the meaning given such
21 term in section 1092(a)(7) of the National Defense
22 Authorization Act for Fiscal Year 2017 (6 U.S.C.
23 223(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).”.

1 **SEC. 411. AIR AND MARINE OPERATIONS FLIGHT HOURS.**

2 (a) INCREASED FLIGHT HOURS.—The Secretary of
3 Homeland Security shall ensure that not fewer than
4 95,000 annual flight hours are carried out by Air and Ma-
5 rine Operations of U.S. Customs and Border Protection.

6 (b) UNMANNED AERIAL SYSTEM.—The Secretary of
7 Homeland Security, after coordination with the Adminis-
8 trator of the Federal Aviation Administration, shall ensure
9 that Air and Marine Operations operate unmanned aerial
10 systems on the southern border of the United States for
11 not less than 24 hours per day for 5 days per week.

12 (c) CONTRACT AIR SUPPORT AUTHORIZATION.—The
13 Commissioner of U.S. Customs and Border Protection
14 may contract for the unfulfilled identified air support mis-
15 sion critical hours, as identified by the Chief of the U.S.
16 Border Patrol.

17 (d) PRIMARY MISSION.—The Commissioner of U.S.
18 Customs and Border Protection shall ensure that—

19 (1) the primary missions for Air and Marine
20 Operations are to directly support U.S. Border Pa-
21 trol activities along the southern border of the
22 United States and Joint Interagency Task Force
23 South operations in the transit zone; and

24 (2) the Executive Assistant Commissioner of
25 Air and Marine Operations assigns the greatest pri-

1 ority to support missions established by the Commis-
2 sioner to carry out the requirements under this Act.

3 (e) HIGH-DEMAND FLIGHT HOUR REQUIREMENTS.—

4 In accordance with subsection (d), the Commissioner of
5 U.S. Customs and Border Protection shall ensure that
6 U.S. Border Patrol Sector Chiefs—

7 (1) identify critical flight hour requirements;

8 and

9 (2) direct Air and Marine Operations to sup-
10 port requests from Sector Chiefs as their primary
11 mission.

12 (f) SMALL UNMANNED AERIAL VEHICLES.—

13 (1) IN GENERAL.—The Chief of the U.S. Bor-
14 der Patrol shall be the executive agent for U.S. Cus-
15 toms and Border Protection's use of small un-
16 manned aerial vehicles for the purpose of meeting
17 the U.S. Border Patrol's unmet flight hour oper-
18 ational requirements and to achieve situational
19 awareness and operational control.

20 (2) COORDINATION.—In carrying out para-
21 graph (1), the Chief of the U.S. Border Patrol
22 shall—

23 (A) coordinate flight operations with the
24 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-

1 tion, or the Chief of the U.S. Border Patrol any authority
2 of the Secretary of Transportation or the Administrator
3 of the Federal Aviation Administration relating to the use
4 of airspace or aviation safety.

5 **SEC. 412. AMENDMENTS TO U.S. CUSTOMS AND BORDER**
6 **PROTECTION.**

7 (a) DUTIES.—Subsection (c) of section 411 of the
8 Homeland Security Act of 2002 (6 U.S.C. 211), as
9 amended by this title, is further amended—

10 (1) in paragraph (20), by striking “and” after
11 the semicolon at the end;

12 (2) by redesignating paragraph (21) as para-
13 graph (23); and

14 (3) by inserting after paragraph (20) the fol-
15 lowing new paragraphs:

16 “(21) administer the U.S. Customs and Border
17 Protection public private partnerships under subtitle
18 G;

19 “(22) administer preclearance operations under
20 the Preclearance Authorization Act of 2015 (19
21 U.S.C. 4431 et seq.; enacted as subtitle B of title
22 VIII of the Trade Facilitation and Trade Enforce-
23 ment Act of 2015; 19 U.S.C. 4301 et seq.); and”.

24 (b) OFFICE OF FIELD OPERATIONS STAFFING.—
25 Subparagraph (A) of section 411(g)(5) of the Homeland

1 Security Act of 2002 (6 U.S.C. 211(g)(5)) is amended by
2 inserting before the period at the end the following: “com-
3 pared to the number indicated by the current fiscal year
4 work flow staffing model”.

5 (c) IMPLEMENTATION PLAN.—Subparagraph (B) of
6 section 814(e)(1) of the Preclearance Authorization Act
7 of 2015 (19 U.S.C. 4433(e)(1); enacted as subtitle B of
8 title VIII of the Trade Facilitation and Trade Enforce-
9 ment Act of 2015; 19 U.S.C. 4301 et seq.) is amended
10 to read as follows:

11 “(B) a port of entry vacancy rate which
12 compares the number of officers identified in
13 subparagraph (A) with the number of officers
14 at the port at which such officer is currently as-
15 signed.”.

16 (d) DEFINITION.—Subsection (r) of section 411 of
17 the Homeland Security Act of 2002 (6 U.S.C. 211) is
18 amended—

19 (1) by striking “this section, the terms” and in-
20 serting the following: “this section:

21 “(1) the terms”;

22 (2) in paragraph (1), as added by subparagraph
23 (A), by striking the period at the end and inserting
24 “; and”; and

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

3 “(2) the term ‘unmanned aerial systems’ has
4 the meaning given the term ‘unmanned aircraft sys-
5 tem’ in section 44801 of the FAA Modernization
6 and Reform Act of 2018 (Public Law 115–254; 49
7 U.S.C. 40101 note).”.

8 **SEC. 413. CONTINUOUS SCREENING BY U.S. CUSTOMS AND**
9 **BORDER PROTECTION.**

10 (a) **IN GENERAL.**—Subtitle B of title IV of the
11 Homeland Security Act of 2002 (6 U.S.C. 211 et seq.),
12 as amended by this title, is further amended by adding
13 at the end the following new section:

14 **“SEC. 420A. CONTINUOUS SCREENING.**

15 “The Commissioner of U.S. Customs and Border
16 Protection shall, in a risk based manner, continuously
17 screen individuals issued any visa, and individuals who are
18 nationals of a program country pursuant to section 217
19 of the Immigration and Nationality Act (8 U.S.C. 1187),
20 who are present, or are expected to arrive within 30 days,
21 in the United States, against the appropriate criminal, na-
22 tional security, and terrorism databases maintained by the
23 Federal Government.”.

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

1 amended by inserting after the item relating to section
2 420, as added by this title, the following new item:

“Sec. 420A. Continuous screening by U.S. Customs and Border Protection.”.

3 **SEC. 414. CUSTOMS TRADE PARTNERSHIP AGAINST TER-**
4 **RORISM.**

5 (a) IN GENERAL.—Subtitle B of title II of the Secu-
6 rity and Accountability for Every Port Act of 2006 (6
7 U.S.C. 961 et seq.) is amended to read as follows:

8 **“Subtitle B—Customs Trade**
9 **Partnership Against Terrorism**

10 **“SEC. 211. ESTABLISHMENT OF THE CUSTOMS TRADE**
11 **PARTNERSHIP AGAINST TERRORISM PRO-**
12 **GRAM.**

13 “(a) IN GENERAL.—There is established within U.S.
14 Customs and Border Protection a voluntary government-
15 private sector partnership program to be known as the
16 Customs Trade Partnership Against Terrorism (CTPAT).

17 “(b) PURPOSE.—The purposes of the CTPAT pro-
18 gram are to—

19 “(1) strengthen and improve the overall secu-
20 rity of the international supply chain and United
21 States border security;

22 “(2) facilitate the movement of secure cargo
23 through the international supply chain;

24 “(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

1 may be, in consultation with the Commercial Cus-
2 toms Operations Advisory Committee established
3 under section 109 of the Trade Facilitation and
4 Trade Enforcement Act of 2015 (Public Law 114–
5 125; 19 U.S.C. 4316);

6 “(2) determine operational feasibility and,
7 where appropriate, provide best practices for meet-
8 ing such new or updated security criteria to CTPAT
9 program participants specific to their entity type;

10 “(3) conduct a phased implementation of such
11 proposed new or updated security criteria; and

12 “(4) provide CTPAT program participants and
13 other interested parties a 90-day comment period to
14 review and comment on such proposed new or up-
15 dated security criteria.

16 “(f) WAIVER.—The Commissioner may waive the re-
17 quirements of subsection (e) if the Commissioner deter-
18 mines there is a significant and imminent risk to the na-
19 tional security of the United States and such a waiver is
20 necessary to protect such national security. Not later than
21 120 days after the issuance of any such waiver, the Com-
22 missioner shall announce on the U.S. Customs and Border
23 Protection website and through other appropriate online
24 publication the Commissioner’s intent to either withdraw
25 such waiver or maintain such waiver while commencing

1 efforts to establish new or updated security criteria in ac-
2 cordance with subsection (c) or (d), respectively.

3 **“SEC. 214. BENEFITS FOR CTPAT PROGRAM PARTICIPANTS.**

4 “(a) IN GENERAL.—The Executive Assistant Com-
5 missioner shall extend certain benefits to each CTPAT
6 program participant. Minimum benefits for each such par-
7 ticipant shall include the following:

8 “(1) Assignment of a U.S. Customs and Border
9 Protection Supply Chain Security Specialist.

10 “(2) Access to the CTPAT program’s web-
11 based Portal system, training materials, and a mech-
12 anism by which to verify other CTPAT program
13 participants’ CTPAT status.

14 “(3) Timely supply chain threat alerts cat-
15 egorized by CTPAT program participant entity type,
16 and an annual and unclassified update made avail-
17 able in such web-based Portal system regarding re-
18 gional and other relevant threats to the international
19 supply chain.

20 “(b) ANNUAL ASSESSMENT.—

21 “(1) IN GENERAL.—The Executive Assistant
22 Commissioner shall conduct, on an annual basis, an
23 assessment of the benefits conferred to CTPAT pro-
24 gram participants by tier and entity type. The Exec-
25 utive Assistant Commissioner shall determine a

1 process to carry out such assessments, including
2 projected milestones and completion dates for ad-
3 dressing data reliability issues and, as necessary,
4 correcting data weaknesses, in order that U.S. Cus-
5 toms and Border Protection can produce accurate
6 and reliable annual assessments that can be com-
7 pared year-to-year.

8 “(2) ELEMENTS.—Each annual assessment
9 conducted pursuant to paragraph (1) shall at a min-
10 imum include the following:

11 “(A) The average reduced security exam
12 rate by CTPAT program participant tier and
13 entity type.

14 “(B) The average reduction in penalties
15 for CTPAT program participants by tier and
16 entity type.

17 “(C) The average reduction in risk assess-
18 ment for CTPAT program participants by tier
19 and entity type.

20 “(3) PUBLIC AVAILABILITY.—The Executive
21 Assistant Commissioner shall make each annual as-
22 sessment publicly available on the CTPAT portal for
23 at least one year.

24 “(c) CONSULTATION.—When assessing benefits in ac-
25 cordance 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-

1 sioner shall issue a determination not later than 90
2 days after such appeal is filed.

3 “(2) APPEALS OF OTHER DECISIONS.—The
4 Commissioner shall establish a process for a CTPAT
5 program participant to appeal a decision of the Ex-
6 ecutive Assistant Commissioner under subsections
7 (b) and (c). Such appeal shall be filed with the Com-
8 missioner not later than 30 days after the date of
9 such decision, and the Commissioner shall issue a
10 determination not later than 90 days after such ap-
11 peal is filed.

12 **“SEC. 219. VALIDATIONS BY OTHER DHS COMPONENTS.**

13 “(a) IN GENERAL.—The Commissioner may recog-
14 nize regulatory inspections of entities conducted by other
15 components of the Department of Homeland Security as
16 sufficient to constitute validation for CTPAT program
17 participation in cases in which any such component’s in-
18 spection regime is harmonized with validation criteria for
19 the CTPAT program. Such regulatory inspections shall
20 not limit the ability of U.S. Customs and Border Protec-
21 tion to conduct a CTPAT program validation.

22 “(b) REVALIDATION.—Nothing in this section may
23 limit the Commissioner’s ability to require a revalidation
24 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 “(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

1 and track information regarding the status of each
2 CTPAT program participant.

3 “(c) CONFIDENTIAL INFORMATION SAFEGUARDS.—
4 In consultation with the Commercial Customs Operations
5 Advisory Committee established under section 109 of the
6 Trade Facilitation and Trade Enforcement Act of 2015
7 (Public Law 114–125; 19 U.S.C. 4316), the Commis-
8 sioner shall develop and implement procedures to ensure
9 the protection of confidential data collected, stored, or
10 shared with government agencies or as part of the applica-
11 tion, certification, validation, recertification, and revalida-
12 tion processes.

13 “(d) RESOURCE MANAGEMENT STAFFING PLAN.—
14 The Commissioner shall—

15 “(1) develop a staffing plan to recruit and train
16 staff (including a formalized training program) to
17 meet the objectives identified in the five-year stra-
18 tegic plan under subsection (a)(1); and

19 “(2) provide cross-training in post incident
20 trade resumption for the CTPAT Director and other
21 relevant personnel who administer the CTPAT pro-
22 gram.

23 “(e) ENGAGEMENT.—In carrying out the standard-
24 ized process required under subsection (a)(4), the Com-
25 missioner 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-

1 ence on the day before the date of the enactment of
2 this Act.

3 (c) TECHNICAL AND CONFORMING AMENDMENTS.—
4 The Security and Accountability for Every Port Act of
5 2006 is amended—

6 (1) in paragraph (4) of section 2 (6 U.S.C.
7 901), by striking “Commissioner responsible for the
8 United States Customs and Border Protection” and
9 inserting “Commissioner of U.S. Customs and Bor-
10 der Protection”; and

11 (2) in paragraph (2) of section 202(c) (6
12 U.S.C. 942(c)), by striking “C-TPAT” and insert-
13 ing “CTPAT”.

14 (d) CLERICAL AMENDMENTS.—The table of contents
15 in section 1(b) of the Security and Accountability for
16 Every Port Act of 2006 is amended by striking the items
17 relating to subtitle B of title II and inserting the following
18 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.”.

1 **SEC. 415. STRATEGY TO ENSURE DETECTION OF ALL**
2 **OPIOID PURITY LEVELS AT PORTS OF ENTRY.**

3 (a) IN GENERAL.—Not later than 180 days after the
4 date of the enactment of this section, the Commissioner
5 of U.S. Customs and Border Protection (CBP) shall—

6 (1) implement a strategy to ensure deployed
7 chemical screening devices are able to identify, in an
8 operational environment, narcotics at purity levels
9 less than or equal to 10 percent, or provide ports of
10 entry with an alternate method for identifying nar-
11 cotics at lower purity levels; and

12 (2) require testing of any new chemical screen-
13 ing devices to understand the abilities and limita-
14 tions of such devices relating to identifying narcotics
15 at various purity levels before CBP commits to the
16 acquisition of such devices.

17 (b) PLAN TO ENSURE OPIOID DETECTION EQUIP-
18 MENT RESILIENCY.—Not later than 180 days after the
19 date of the enactment of this section, the Secretary of
20 Homeland Security shall implement a plan for the long-
21 term development of a centralized spectral database for
22 chemical screening devices. Such plan shall address the
23 following:

24 (1) How newly identified spectra will be col-
25 lected, stored, and distributed to such devices in

1 their operational environment, including at ports of
2 entry.

3 (2) Identification of parties responsible for up-
4 dates and maintenance of such database.

5 **SEC. 416. AUTHORIZATION OF THE IMMIGRATION ADVI-**
6 **SORY PROGRAM.**

7 (a) IN GENERAL.—Subtitle B of title IV of the
8 Homeland Security Act of 2002 (6 U.S.C. 211 et seq.),
9 as amended by this title, is further amended by adding
10 at the end the following new section:

11 **“SEC. 420B. IMMIGRATION ADVISORY PROGRAM.**

12 “(a) IN GENERAL.—There is authorized within U.S.
13 Customs and Border Protection an immigration advisory
14 program (in this section referred to as the ‘program’) for
15 United States Customs and Border Protection officers,
16 pursuant to an agreement with a host country, to assist
17 air carriers and security employees at foreign airports with
18 review of traveler information during the processing of
19 flights bound for the United States.

20 “(b) ACTIVITIES.—In carrying out the program, U.S.
21 Customs and Border Protection officers may—

22 “(1) be present during processing of flights
23 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 “(1) a copy of such agreement, which shall in-
2 clude—

3 “(A) the identification of the host country
4 with which United States Customs and Border
5 Protection intends to enter into such agree-
6 ment;

7 “(B) the location at which activities de-
8 scribed in subsection (b) will be conducted pur-
9 suant to such agreement; and

10 “(C) the terms and conditions for United
11 States Customs and Border Protection per-
12 sonnel operating at such location;

13 “(2) country-specific information on the antici-
14 pated homeland security benefits associated with
15 such agreement;

16 “(3) an assessment of the impacts such agree-
17 ment will have on United States Customs and Bor-
18 der Protection domestic port of entry staffing;

19 “(4) information on the anticipated costs over
20 the 5 fiscal years after such agreement enters into
21 force associated with carrying out such agreement;

22 “(5) details on information sharing mechanisms
23 to ensure that United States Customs and Border
24 Protection has current information to prevent ter-
25 rorist and criminal travel; and

1 “(6) other factors that the Commissioner deter-
2 mines necessary for Congress to comprehensively as-
3 sess the appropriateness of carrying out the pro-
4 gram.

5 “(d) AMENDMENT OF EXISTING AGREEMENTS.—Not
6 later than 30 days before a substantially amended pro-
7 gram agreement with the government of a host country
8 in effect as of the date of the enactment of this section
9 enters into force, the Commissioner of U.S. Customs and
10 Border Protection shall provide to the Committee on
11 Homeland Security of the House of Representatives and
12 the Committee on Homeland Security and Governmental
13 Affairs of the Senate—

14 “(1) a copy of such agreement, as amended;
15 and

16 “(2) the justification for such amendment.

17 “(e) DEFINITIONS.—In this section, the terms ‘air
18 carrier’ and ‘foreign air carrier’ have the meanings given
19 such terms in section 40102 of title 49, United States
20 Code.”.

21 (b) CONFORMING AMENDMENT.—Subsection (c) of
22 section 411 of the Homeland Security Act of 2002 (6
23 U.S.C. 211), as amended by this title, is further amend-
24 ed—

1 (1) in paragraph (22), by striking “and” after
2 the semicolon at the end;

3 (2) by redesignating paragraph (23) as para-
4 graph (24); and

5 (3) by inserting after paragraph (22) the fol-
6 lowing new paragraph:

7 “(23) carry out section 420B, relating to the
8 immigration advisory program; and”.

9 (c) CLERICAL AMENDMENT.—The table of contents
10 in section 1(b) of the Homeland Security Act of 2002 is
11 amended by inserting after the item relating to section
12 420A, as added by this title, the following new item:

“Sec.420B. Immigration advisory program.”.

13 **SEC. 417. BORDER SECURITY TECHNOLOGY ACCOUNT-**
14 **ABILITY.**

15 (a) IN GENERAL.—Subtitle C of title IV of the
16 Homeland Security Act of 2002 (6 U.S.C. 231 et seq.)
17 is amended by adding at the end the following new section:

18 **“SEC. 437. BORDER SECURITY TECHNOLOGY PROGRAM**
19 **MANAGEMENT.**

20 “(a) PLANNING DOCUMENTATION.—For each border
21 security technology acquisition program of the Depart-
22 ment that is determined to be a major acquisition pro-
23 gram, 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.”.

1 **SEC. 418. ESTABLISHMENT OF U.S. IMMIGRATION AND CUS-**
2 **TOMS ENFORCEMENT.**

3 (a) IN GENERAL.—Section 442 of the Homeland Se-
4 curity Act of 2002 (6 U.S.C. 252) is amended to read
5 as follows:

6 **“SEC. 442. U.S. IMMIGRATION AND CUSTOMS ENFORCE-**
7 **MENT.**

8 “(a) ESTABLISHMENT.—There is established within
9 the Department an agency to be known as U.S. Immigra-
10 tion and Customs Enforcement.

11 “(b) DIRECTOR OF U.S. IMMIGRATION AND CUSTOMS
12 ENFORCEMENT.—There shall be at the head of U.S. Im-
13 migration and Customs Enforcement a Director of U.S.
14 Immigration and Customs Enforcement (in this section re-
15 ferred to as the ‘Director’).

16 “(c) DUTIES AND QUALIFICATIONS.—The Director
17 shall—

18 “(1) have a minimum of five years—

19 “(A) professional experience in law en-
20 forcement, which may include law enforcement
21 as it relates to the immigration laws, as defined
22 in paragraph (17) of section 101(a) of the Im-
23 migration and Nationality Act (8 U.S.C.
24 1101(a)(17)) or the customs and trade laws of
25 the United States, as defined in section 2 of the

1 Trade Facilitation and Trade Enforcement Act
2 of 2015 (19 U.S.C. 4301); and

3 “(B) management experience;

4 “(2) in coordination with U.S. Customs and
5 Border Protection and United States Citizenship
6 and Immigration Services, enforce and administer
7 immigration laws, as defined in paragraph (17) of
8 section 101(a) of the Immigration and Nationality
9 Act (8 U.S.C. 1101(a)), including the identification,
10 arrest, detention, and removal of aliens who may be
11 inadmissible to, or deportable from, the United
12 States;

13 “(3) have the authority to investigate and,
14 where appropriate, refer for prosecution, any crimi-
15 nal or civil violation of Federal law relating to or in-
16 volving—

17 “(A) border control and security, including
18 the prevention of the entry or residence of ter-
19 rorists, criminals, and human rights violators;

20 “(B) the customs and trade laws of the
21 United States, as defined in section 2 of the
22 Trade Facilitation and Trade Enforcement Act
23 of 2015 (19 U.S.C. 4301);

24 “(C) fraud, false statements, or other vio-
25 lations on the import or export of merchandise,

1 including the illicit possession, movement of, or
2 trade in goods, services, property, arms, instru-
3 ments of terrorism, items controlled or prohib-
4 ited from export, goods made with forced or in-
5 dentured labor, intellectual property, or cur-
6 rency or other monetary instruments;

7 “(D) bulk cash smuggling or other finan-
8 cial crimes with a cross-border or international
9 nexus;

10 “(E) the immigration laws, as defined in
11 paragraph (17) of section 101(a) of the Immi-
12 gration and Nationality Act (8 U.S.C. 1101(a));

13 “(F) transnational organized crime;

14 “(G) chapter 40 or 44 of title 18, United
15 States Code, or other violation relating to explo-
16 sives, firearms, other destructive devices involv-
17 ing an alien;

18 “(H) severe forms of trafficking in per-
19 sons, as defined in section 103 of the Victims
20 of Trafficking and Violence Protection Act of
21 2000 (22 U.S.C. 7102);

22 “(I) the production, procurement, counter-
23 feiting, alteration, or use of fraudulent immi-
24 gration documents or fraudulently obtaining im-
25 migration benefits;

1 “(J) unlawful use of personal information,
2 when such use relates to or affects border secu-
3 rity, terrorism, customs, immigration, natu-
4 ralization, trade, or transportation security;

5 “(K) computer crimes, pursuant to section
6 1030(d) of title 18, United States Code, in co-
7 operation, where required by law, with the
8 United States Secret Service and the Federal
9 Bureau of Investigation;

10 “(L) drug laws, as specified in the Con-
11 trolled Substances Act and the Controlled Sub-
12 stances Import and Export Act in the context
13 of cross-border criminal activity;

14 “(M) child exploitation, child pornography,
15 or traveling child sex offenders pursuant to sec-
16 tion 890A(b)(2)(A) of the Homeland Security
17 Act of 2002 (6 U.S.C. 473(b)(2)(A)); and

18 “(N) cyber-enabled crimes pursuant to sec-
19 tion 890A(d)(2)(B) of the Homeland Security
20 Act of 2002 (6 U.S.C. 473(d)(2)(B));

21 “(4) administer the National Intellectual Prop-
22 erty Rights Coordination Center established in sec-
23 tion 305 of the Trade Facilitation and Trade En-
24 forcement Act of 2015 (Public Law 114–125; 19
25 U.S.C. 4344);

1 “(5) jointly with the Commissioner of U.S. Cus-
2 toms and Border Protection, develop and submit the
3 joint strategic plan required under section 105 of
4 the Trade Facilitation and Trade Enforcement Act
5 of 2015 (Public Law 114–125; 19 U.S.C. 4314);

6 “(6) coordinate, as otherwise permitted by law,
7 with Federal, State, local, tribal, and foreign agen-
8 cies in carrying out the duties set forth in para-
9 graphs (2) and (3);

10 “(7) in coordination with the Office of Inter-
11 national Affairs of the Department and the Depart-
12 ment of State, establish staff liaison offices and vet-
13 ted units in foreign countries to support law enforce-
14 ment activities that require international coopera-
15 tion, including investigations and repatriation ef-
16 forts;

17 “(8) assign employees of the Department to
18 diplomatic and consular posts, in coordination with
19 the Secretary, pursuant to section 428(e);

20 “(9) authorize danger pay allowance for em-
21 ployees of the Department pursuant to section 5928
22 of title 5, United States Code, with the approval of
23 the Secretary of State;

24 “(10) provide technical assistance and training
25 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

1 and appropriate medical care and dental and
2 mental health services to detained aliens in the
3 custody of the agency;

4 “(D) plan, coordinate, and manage the
5 execution of exclusion, deportation, and removal
6 orders issued to aliens;

7 “(E) investigate and refer for prosecution
8 any civil or criminal violation of the immigra-
9 tion laws or any offense described in section
10 287(a)(5) of the Immigration and Nationality
11 Act (8 U.S.C. 1357(a)(5)); and

12 “(F) carry out other duties and powers
13 prescribed by the Director.

14 “(h) OFFICE OF THE PRINCIPAL LEGAL ADVISOR.—

15 “(1) IN GENERAL.—There is established in
16 U.S. Immigration and Customs Enforcement the Of-
17 fice of the Principal Legal Advisor.

18 “(2) PRINCIPAL LEGAL ADVISOR.—There shall
19 be at the head of the Office the Principal Legal Ad-
20 visor a Principal Legal Advisor.

21 “(3) DUTIES.—The Office of the Principal
22 Legal Advisor shall—

23 “(A) provide specialized legal advice to the
24 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

1 review of U.S. Immigration and Custom En-
2 forcement's organizational health, effectiveness,
3 and efficiency of mission;

4 “(C) provide and manage the security pro-
5 grams and operations for U.S. Immigration and
6 Customs Enforcement; and

7 “(D) carry out other duties and powers
8 prescribed by the Director.

9 “(j) OFFICE OF MANAGEMENT AND ADMINISTRA-
10 TION.—

11 “(1) IN GENERAL.—There is established in
12 U.S. Immigration and Customs Enforcement the Of-
13 fice of Management and Administration.

14 “(2) EXECUTIVE ASSOCIATE DIRECTOR.—There
15 shall be at the head of the Office of Management
16 and Administration an Executive Associate Director,
17 who shall report to the Director.

18 “(3) DUTIES.—The Office of Management and
19 Administration shall—

20 “(A) oversee and execute the agency's ad-
21 ministrative and management support functions
22 to ensure compliance with all laws, regulations
23 and policies, sound resource and asset manage-
24 ment, internal controls, and in furtherance of
25 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

1 such Act as of the date of the enactment of such
2 Act. In addition to the functions, missions, duties,
3 and authorities specified in such amended section
4 442, U.S. Immigration and Customs Enforcement
5 shall continue to perform and carry out the func-
6 tions, missions, duties, and authorities under section
7 442 of such Act as in existence on the day before
8 such date of enactment (notwithstanding the treat-
9 ment described in this paragraph).

10 (2) RULES OF CONSTRUCTION.—

11 (A) RULES AND REGULATIONS.—Notwith-
12 standing the treatment described in paragraph
13 (1), nothing in this Act may be construed as af-
14 fecting in any manner any rule or regulation
15 issued or promulgated pursuant to any provi-
16 sion of law, including section 442 of the Home-
17 land Security Act of 2002, as in existence on
18 the day before the date of the enactment of this
19 Act, and any such rule or regulation shall con-
20 tinue to have full force and effect on and after
21 such date.

22 (B) OTHER ACTIONS.—Notwithstanding
23 the treatment described in paragraph (1), noth-
24 ing in this Act may be construed as affecting in
25 any manner any action, determination, policy,

1 or decision pursuant to section 442 of the
2 Homeland Security Act of 2002 as in existence
3 on the day before the date of the enactment of
4 this Act, and any such action, determination,
5 policy, or decision shall continue to have full
6 force and effect on and after such date.

7 (c) CONTINUATION IN OFFICE.—

8 (1) DIRECTOR.—The individual serving as the
9 Director of U.S. Immigration and Customs Enforce-
10 ment on the day before the date of the enactment
11 of this Act (notwithstanding the treatment described
12 in subsection (b)(1)) may serve as the Director of
13 U.S. Immigration and Customs Enforcement in ac-
14 cordance with section 442 of the Homeland Security
15 Act of 2002, as amended by subsection (a), until the
16 earlier of—

17 (A) the date on which such individual is no
18 longer eligible to serve as Director; or

19 (B) the date on which a person nominated
20 by the President to be the Director is confirmed
21 by the Senate in accordance with such section
22 441.

23 (2) OTHER POSITIONS.—The individuals serv-
24 ing as the Deputy Director, Executive Associate Di-
25 rectors, Deputy Executive Associate Directors, or

1 similar officers or officials of U.S. Immigration and
2 Customs Enforcement under section 442 of the
3 Homeland Security Act of 2002 on the day before
4 the date of the enactment of this Act (notwith-
5 standing the treatment described in subsection
6 (b)(1)) may serve as the appropriate Deputy Direc-
7 tor, Executive Associate Directors, Deputy Executive
8 Associate Directors, Associate Directors, Deputy As-
9 sociate Directors, Assistant Directors, and other of-
10 ficers and officials under section 442 of such Act, as
11 amended by subsection (a), unless the individual
12 serving as the Director of U.S. Immigration and
13 Customs Enforcement determines that another indi-
14 vidual should hold such position.

15 (d) TRANSPORTATION.—Paragraph (6) of section
16 1344(b) of title 31, United States Code, is amended by
17 inserting “, the Director of U.S. Immigration and Cus-
18 toms Enforcement, the Commissioner of Customs and
19 Border Protection,” before “the Administrator of the
20 Drug Enforcement Administration,”.

21 (e) CONFORMING AMENDMENTS.—

22 (1) TITLE 5.—Section 5314 of title 5, United
23 States Code, is amended by inserting after “Director
24 of the Bureau of Citizenship and Immigration Serv-

1 ices.” the following new item: “Director of U.S. Im-
2 migration and Customs Enforcement.”.

3 (2) TITLE 18.—Subsection (d) of section 1030
4 of title 18, United States Code, is amended—

5 (A) in paragraph (1), by inserting “and
6 U.S. Immigration and Customs Enforcement”
7 after “United States Secret Service”;

8 (B) in paragraph (2), by inserting, “, in
9 collaboration with U.S. Immigration andcus-
10 toms Enforcement” after “Federal Bureau of
11 Investigation”; and

12 (C) in paragraph (3), by striking “Sec-
13 retary of the Treasury” and inserting “Sec-
14 retary of Homeland Security”.

15 (3) TRADE FACILITATION AND TRADE EN-
16 FORCEMENT ACT OF 2015.—Paragraph (2) of section
17 802(d) of the Trade Facilitation and Trade Enforce-
18 ment Act of 2015 (Public Law 114–125) is amended
19 by inserting before the period at the end the fol-
20 lowing: “or the Director of U.S. Immigration and
21 Customs Enforcement, as determined by the Sec-
22 retary of Homeland Security”.

23 (4) HOMELAND SECURITY ACT OF 2002.—Title
24 IV of the Homeland Security Act of 2002 is amend-
25 ed—

1 (A) in subtitle C—

2 (i) in subsection (e) of section 428 (6
3 U.S.C. 236), by adding at the end the fol-
4 lowing new paragraph:

5 “(9) DELEGATED AUTHORITY.—For purposes
6 of this subsection, the Secretary shall act through
7 the Director of U.S. Immigration and Customs En-
8 forcement.”; and

9 (ii) in section 432 (6 U.S.C. 240)—

10 (I) by redesignating subsection
11 (e) as subsection (f); and

12 (II) by inserting after subsection
13 (d) the following new subsection:

14 “(e) ADMINISTRATION.—The Director of U.S. Immi-
15 gration and Customs Enforcement shall administer BEST
16 units established under this section.”;

17 (B) in subtitle D—

18 (i) by amending the subtitle heading
19 to read as follows: “**U.S. Immigration**
20 **and Customs Enforcement**”; and

21 (ii) by repealing sections 445 and 446
22 (6 U.S.C. 255 and 256);

23 (C) in subtitle E—

24 (i) in subsection (a)(2)(C) of section
25 451 (6 U.S.C. 271), by striking “at the

1 same level as the Assistant Secretary of
2 the Bureau of Border Security” and in-
3 serting “in accordance with section 5314
4 of title 5, United States Code”;

5 (ii) in subsection (c) of section 459 (6
6 U.S.C. 276), by striking “Assistant Sec-
7 retary of the Bureau of Border Security”
8 and inserting “Director of U.S. Immigra-
9 tion and Customs Enforcement”; and

10 (iii) in subsection (b)(2)(A) of section
11 462 (6 U.S.C. 279), in the matter pre-
12 ceding clause (i), by striking “Assistant
13 Secretary of the Bureau of Border Secu-
14 rity” and inserting “Director of U.S. Im-
15 migration and Customs Enforcement”; and

16 (D) in subtitle F, in subsection (a)(2)(B)
17 of section 472 (6 U.S.C. 292), by striking “Bu-
18 reau of Border Security” and inserting “U.S.
19 Immigration and Customs Enforcement”.

20 (f) CLERICAL AMENDMENTS.—The table of contents
21 in section 1(b) of such Act is amended—

22 (1) by striking the item relating to subtitle D
23 of title IV and inserting the following new item:

1 **“Subtitle D—U.S. Immigration and**
2 **Customs Enforcement”.**; and

3 (2) by striking the items relating sections 445
4 and 446.

5 **SEC. 419. BIOMETRIC IDENTIFICATION TRANSNATIONAL**
6 **MIGRATION ALERT PROGRAM.**

7 (a) IN GENERAL.—Subtitle D of title IV of the
8 Homeland Security Act of 2002 (6 U.S.C. 251 et seq.),
9 as amended by this title, is further amended by adding
10 at the end the following new section:

11 **“SEC. 445. BIOMETRIC IDENTIFICATION TRANSNATIONAL**
12 **MIGRATION ALERT PROGRAM.**

13 “(a) ESTABLISHMENT.—There is established in the
14 Department a program to be known as the ‘Biometric
15 Identification Transnational Migration Alert Program’
16 (referred to in this section as ‘BITMAP’) to address and
17 reduce national security, border security, and terrorist
18 threats before such threats reach the international border
19 of the United States.

20 “(b) DUTIES.—In carrying out BITMAP operations,
21 the Secretary, acting through the Director of U.S. Immi-
22 gration and Customs Enforcement, shall—

23 “(1) coordinate, in consultation with the Sec-
24 retary of State, appropriate representatives of for-
25 eign 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;

1 “(C) the Department of Defense Auto-
2 mated Biometric Identification System (com-
3 monly known as ‘ABIS’), or successor database;

4 “(D) the Department’s Automated Biomet-
5 ric Identification System (commonly known as
6 ‘IDENT’), or successor database; and

7 “(E) any other database, notice, or means
8 that the Secretary, in consultation with the
9 heads of other Federal departments and agen-
10 cies responsible for such databases, notices, or
11 means, designates;

12 “(4) provide partner countries with training,
13 guidance, and best practices recommendations re-
14 garding the enrollment of individuals in BITMAP;
15 and

16 “(5) ensure biometric and biographic identifica-
17 tion data collected pursuant to BITMAP are incor-
18 porated into appropriate United States Government
19 databases, in compliance with the policies and proce-
20 dures established by the Privacy Officer appointed
21 under section 222.

22 “(c) COLLABORATION.—The Secretary shall ensure
23 that BITMAP operations include participation from rel-
24 evant components of the Department, and request partici-
25 pation 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-

1 ate with a copy of such agreement or arrangement to es-
2 tablish such operations, including the following:

3 “(1) The identification of the foreign country
4 with which the Secretary intends to enter into such
5 an agreement or arrangement.

6 “(2) The location at which such operations will
7 be conducted.

8 “(3) Goals for BITMAP operations in the for-
9 eign country.

10 “(4) The terms and conditions for Department
11 personnel operating at such location.

12 “(f) CAPTURED INFORMATION OF UNITED STATES
13 CITIZENS.—The Secretary shall ensure that any biometric
14 and biographic identification data of United States citi-
15 zens that is captured by BITMAP operations is expunged
16 from all databases to which such data was uploaded, un-
17 less such data is retained for specific law enforcement or
18 intelligence purposes.”.

19 (b) REPORT.—Not later than 180 days after the date
20 on which the Biometric Identification Transnational Mi-
21 gration Alert Program (BITMAP) is established under
22 section 447 of the Homeland Security Act of 2002 (as
23 added by subsection (a) of this section) and annually
24 thereafter for the following five years, the Secretary of
25 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;

1 (8) includes a review of the redress process for
2 BITMAP; and

3 (9) details the effectiveness of BITMAP oper-
4 ations in enhancing national security, border secu-
5 rity, and counterterrorism operations.

6 (c) BRIEFINGS.—Not later than 30 days after each
7 report is submitted pursuant to subsection (b), the Sec-
8 retary of Homeland Security shall brief the Committee on
9 Homeland Security and Governmental Affairs of the Sen-
10 ate and the Committee on Homeland Security of the
11 House of Representatives regarding—

12 (1) individuals enrolled in BITMAP who have
13 been apprehended at the United States border or in
14 the interior of the United States; and

15 (2) asylum claims that were submitted by indi-
16 viduals who are enrolled in BITMAP.

17 (d) CLERICAL AMENDMENT.—The table of contents
18 in section 1(b) of the Homeland Security Act of 2002 is
19 amended by inserting after the item relating to section
20 444 the following new item:

“Sec. 445. Biometric Identification Transnational Migration Alert Program.”.

21 **SEC. 420. REPORTING OF VISA OVERSTAYS.**

22 Section 2 of Public Law 105–173 (8 U.S.C. 1376)
23 is amended—

24 (1) in subsection (a)—

1 (A) by striking “Attorney General” and in-
2 serting “Secretary of Homeland Security”; and

3 (B) by inserting before the period at the
4 end the following: “, and any additional infor-
5 mation that the Secretary determines necessary
6 for purposes of the report under subsection
7 (b)”;

8 (2) by amending subsection (b) to read as fol-
9 lows:

10 “(b) ANNUAL REPORT.—Not later than September
11 30, 2021, and not later than September 30 of each year
12 thereafter, the Secretary of Homeland Security shall sub-
13 mit to the Committee on Homeland Security and the Com-
14 mittee on the Judiciary of the House of Representatives
15 and to the Committee on Homeland Security and Govern-
16 mental Affairs and the Committee on the Judiciary of the
17 Senate a report providing, for the preceding fiscal year,
18 numerical estimates (including information on the meth-
19 odology utilized to develop such numerical estimates) of
20 the following:

21 “(1) For each country, the number of aliens
22 from the country who are described in subsection
23 (a), including the following:

24 “(A) The total number of such aliens with-
25 in all classes of nonimmigrant aliens described

1 in section 101(a)(15) of the Immigration and
2 Nationality Act (8 U.S.C. 1101(a)(15)).

3 “(B) The number of such aliens within
4 each of the classes of nonimmigrant aliens, as
5 well as the number of such aliens within each
6 of the subclasses of such classes of non-
7 immigrant aliens, as applicable.

8 “(2) For each country, the percentage of the
9 total number of aliens from the country who were
10 present in the United States and were admitted to
11 the United States as nonimmigrants who are de-
12 scribed in subsection (a).

13 “(3) The number of aliens described in sub-
14 section (a) who arrived by land at a port of entry
15 into the United States.

16 “(4) The number of aliens described in sub-
17 section (a) who entered the United States using a
18 border crossing identification card (as such term is
19 defined in section 101(a)(6) of the Immigration and
20 Nationality Act (8 U.S.C. 1101(a)(6))).

21 “(5) The number of Canadian nationals who
22 entered the United States without a visa whose au-
23 thorized period of stay in the United States termi-
24 nated during the previous fiscal year, but who re-
25 mained in the United States.”.

1 **SEC. 421. STUDENT AND EXCHANGE VISITOR INFORMATION**
2 **SYSTEM VERIFICATION.**

3 Not later than 90 days after the date of the enact-
4 ment of this Act, the Secretary of Homeland Security shall
5 ensure that the information collected under the program
6 established under section 641 of the Illegal Immigration
7 Reform and Immigrant Responsibility Act of 1996 (8
8 U.S.C. 1372) is available to officers of U.S. Customs and
9 Border Protection for the purpose of conducting primary
10 inspections of aliens seeking admission to the United
11 States at each port of entry of the United States.

12 **SEC. 422. SOCIAL MEDIA REVIEW OF VISA APPLICANTS.**

13 (a) IN GENERAL.—Subtitle D of title IV of the
14 Homeland Security Act of 2002 (6 U.S.C. 231 et seq.),
15 as amended by this title, is further amended by adding
16 at the end the following new sections:

17 **“SEC. 446. SOCIAL MEDIA SCREENING.**

18 “(a) IN GENERAL.—Not later than 180 days after
19 the date of the enactment of this section, the Secretary
20 shall, to the greatest extent practicable, and in a risk
21 based manner and on an individualized basis, begin re-
22 viewing the social media accounts of certain visa appli-
23 cants who are citizens of, or who reside in, high-risk coun-
24 tries, as determined by the Secretary based on the criteria
25 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

1 individual, the Secretary of Health and Human
2 Services shall provide to the Secretary of Homeland
3 Security any disclosed gang affiliation information
4 the unaccompanied alien child provided to the De-
5 partment of Health and Human Services, including
6 factual information provided by employees and con-
7 tractors of the Department related to patterns of
8 violent behavior or suspected gang affiliation while
9 under their supervision.

10 “(2) PROVIDED TO THE NATIONAL GANG
11 UNIT.—The Secretary of Homeland Security shall
12 share the information provided pursuant to para-
13 graph (1) with relevant National Gang Unit task
14 force units.

15 “(e) EFFECTIVE DATE.—This section shall apply to
16 any unaccompanied alien child apprehended on or after
17 the date of the enactment of this section.

18 “(f) AUTHORIZATION OF APPROPRIATIONS.—There
19 is authorized to be appropriated \$5,000,000 for each of
20 fiscal years 2021 and 2022 to carry out this section.”.

21 (b) CLERICAL AMENDMENT.—The table of contents
22 in section 1(b) of the Homeland Security Act of 2002 is
23 amended by inserting after the item relating to section
24 447, as added by this title, the following new item:

“Sec. 448. National Gang Unit.”.

1 **SEC. 424. HOMELAND SECURITY INVESTIGATIONS**
2 **TRANSNATIONAL CRIMINAL INVESTIGATIVE**
3 **UNITS.**

4 (a) IN GENERAL.—Subtitle D of title IV of the
5 Homeland Security Act of 2002 (6 U.S.C. 231 et seq.),
6 as amended by this title, is further amended by adding
7 at the end the following new section:

8 **“SEC. 449. TRANSNATIONAL CRIMINAL INVESTIGATIVE**
9 **UNITS.**

10 “(a) ESTABLISHMENT.—There is established within
11 the Department a program, which shall be known as the
12 ‘Homeland Security Investigations Transnational Crimi-
13 nal Investigative Unit Program’ (referred to in this section
14 as ‘TCIU Program’). The TCIU Program shall be headed
15 by an Assistant Director, who shall be appointed by the
16 Executive Associate Director of U.S. Immigration and
17 Customs Enforcement, Homeland Security Investigations.

18 “(b) PURPOSE.—The purpose of the TCIU Program
19 shall be to—

20 “(1) lead homeland security investigations into
21 transnational criminal organizations; and

22 “(2) enhance cooperation between Homeland
23 Security Investigations and trusted and vetted for-
24 eign law enforcement partners in order to identify
25 targets, collect evidence, share information, and fa-
26 cilitate the prosecution of transnational criminal or-

1 organizations both in-country and through the United
2 States judicial system.

3 “(c) AUTHORIZATION OF APPROPRIATIONS.—There
4 is authorized to be appropriated, \$5,000,000 for each of
5 fiscal years 2021 and 2022 to carry out this section.”.

6 (b) CLERICAL AMENDMENT.—The table of contents
7 in section 1(b) of the Homeland Security Act of 2002 is
8 amended by inserting after the item relating to section
9 448, as added by this title, the following new item:

“Sec. 449. Transnational criminal investigative unit program.”.

10 **SEC. 425. HOMELAND SECURITY INVESTIGATIONS INNOVA-**
11 **TION LAB.**

12 (a) IN GENERAL.—Subtitle D 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. 450. INNOVATION LAB.**

17 “(a) ESTABLISHMENT.—There is established within
18 the Department a program, which shall be known as the
19 ‘Homeland Security Investigations Innovation Lab’ (re-
20 ferred to in this section as ‘Innovation Lab’. The Inno-
21 vation Lab shall be headed by an Assistant Director, who
22 shall be appointed by the Executive Associate Director of
23 United States Immigration and Customs Enforcement,
24 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.

1 **“SEC. 451. UNITED STATES CITIZENSHIP AND IMMIGRATION**
2 **SERVICES.**

3 “(a) ESTABLISHMENT.—There is established within
4 the Department an agency to be known as United States
5 Citizenship and Immigration Services.

6 “(b) DIRECTOR OF UNITED STATES CITIZENSHIP
7 AND IMMIGRATION SERVICES.—There shall be at the head
8 of United States Citizenship and Immigration Services a
9 Director of United States Citizenship and Immigration
10 Services (in this section referred to as the ‘Director’).

11 “(c) DUTIES AND QUALIFICATIONS.—The Director
12 shall—

13 “(1) have a minimum of five years of manage-
14 ment experience;

15 “(2) establish national immigration services
16 policies and priorities;

17 “(3) meet regularly with the Citizenship and
18 Immigration Services Ombudsman (established in
19 section 452) to correct serious problems identified by
20 such Ombudsman;

21 “(4) advise the Secretary with respect to any
22 policy or operation of United States Citizenship and
23 Immigration Services that may significantly affect
24 another component or office of the Department;

25 “(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-

1 fits and develop systems and techniques for
2 identifying immigration benefit fraud; and

3 “(F) carry out other duties and powers
4 prescribed by the Director.

5 “(k) IMMIGRATION RECORD AND IDENTITY SERV-
6 ICES DIRECTORATE.—

7 “(1) IN GENERAL.—There is established in
8 United States Citizenship and Immigration Services
9 an Immigration Records and Identity Services Di-
10 rectorate.

11 “(2) ASSOCIATE DIRECTOR.—There shall be at
12 the head of the Immigration Records and Identity
13 Services Directorate an Associate Director, who shall
14 report to the Director.

15 “(3) DUTIES.—The Associate Director of the
16 Immigration Records and Identity Services Direc-
17 torate shall—

18 “(A) collect and disseminate biometric in-
19 formation to support the integrity of the immi-
20 gration system;

21 “(B) manage the employment verification
22 system pursuant to 404(a) of the Illegal Immi-
23 gration Reform and Immigrant Responsibility
24 Act of 1996 (8 U.S.C. 1324a note), or suc-
25 cessor 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 “(1) 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

1 States Citizenship and Immigration Services
2 service centers;

3 “(B) conduct security and background in-
4 vestigations of applicants for immigration bene-
5 fits and develop systems and techniques for
6 identifying immigration benefit fraud;

7 “(C) manage the employment creation visa
8 program under section 203(b)(5) of the Immi-
9 gration and Nationality Act (8 U.S.C.
10 1153(b)(5)); and

11 “(D) carry out other duties and powers
12 prescribed by the Director.

13 “(m) OTHER AUTHORITIES.—

14 “(1) IN GENERAL.—The Secretary may estab-
15 lish such other Associate Directors, or other similar
16 positions or officials, as the Secretary determines
17 necessary to carry out the missions, duties, func-
18 tions, and authorities of United States Citizenship
19 and Immigration Services.

20 “(2) NOTIFICATION.—If the Secretary exercises
21 the authority provided pursuant to paragraph (1),
22 the Secretary shall notify the Committee on Home-
23 land Security and the Committee on the Judiciary of
24 the House of Representatives and the Committee on
25 Homeland Security and Governmental Affairs and

1 the Committee on the Judiciary of the Senate not
2 later than 30 days before exercising such author-
3 ity.”.

4 (b) SPECIAL RULES.—

5 (1) TREATMENT.—Section 451 of the Home-
6 land Security Act of 2002 (6 U.S.C. 271), as
7 amended by subsection (a) of this section, shall be
8 treated as if included in such Act as of the date of
9 the enactment of such Act. In addition to the func-
10 tions, missions, duties, and authorities specified in
11 such amended section 451, United States Citizen-
12 ship and Immigration Services shall continue to per-
13 form and carry out the functions, missions, duties,
14 and authorities under section 451 of such Act as in
15 existence on the day before such date of enactment
16 (notwithstanding the treatment described in this
17 paragraph).

18 (2) RULES OF CONSTRUCTION.—

19 (A) RULES AND REGULATIONS.—Notwith-
20 standing the treatment described in paragraph
21 (1), nothing in this Act may be construed as af-
22 fecting in any manner any rule or regulation
23 issued or promulgated pursuant to any provi-
24 sion of law, including section 451 of the Home-
25 land Security Act of 2002 (6 U.S.C. 271), as

1 in existence on the day before the date of the
2 enactment of this Act, and any such rule or
3 regulation shall continue to have full force and
4 effect on and after such date.

5 (B) OTHER ACTIONS.—Notwithstanding
6 the treatment described in paragraph (1), noth-
7 ing in this Act may be construed as affecting in
8 any manner any action, determination, policy,
9 or decision pursuant to section 451 of the
10 Homeland Security Act of 2002 (6 U.S.C. 271)
11 as in existence on the day before the date of the
12 enactment of this Act, and any such action, de-
13 termination, policy, or decision shall continue to
14 have full force and effect on and after such
15 date.

16 (c) CONTINUATION IN OFFICE.—

17 (1) DIRECTOR.—The individual serving as Di-
18 rector of United States Citizenship and Immigration
19 Services on the day before the date of the enactment
20 of this Act may, notwithstanding the treatment pro-
21 vision under paragraph (1) of subsection (b), con-
22 tinue to serve as the Director of United States Citi-
23 zenship and Immigration Services on and after such
24 date of enactment in accordance with section 451 of
25 the Homeland Security Act of 2002 (6 U.S.C. 271),

1 as amended by subsection (a) of this section, until
2 the earlier of—

3 (A) the date on which such individual is no
4 longer eligible to serve as Director; or

5 (B) the date on which a person nominated
6 by the President to be the Director is confirmed
7 by the Senate in accordance with such amended
8 section 451.

9 (2) OTHER POSITIONS.—The individuals serv-
10 ing as Chiefs, Associate Directors and other officers
11 and officials under section 451 of the Homeland Se-
12 curity Act of 2002 (6 U.S.C. 271) on the day before
13 the date of the enactment of this Act may, notwith-
14 standing the treatment provision under paragraph
15 (1) of subsection (b), serve as the appropriate
16 Chiefs, Assistant Directors and other officers and of-
17 ficials under such section 451 as amended by sub-
18 section (a) of this section unless the Director of
19 United States Citizenship and Immigration Services
20 determines that another individual should hold such
21 position.

22 (d) REFERENCES.—

23 (1) TITLE 5.—Section 5314 of title 5, United
24 States Code, is amended by striking “Director of the
25 Bureau of Citizenship and Immigration Services”

1 and inserting “Director of United States Citizenship
2 and Immigration Services, Department of Homeland
3 Security”.

4 (2) OTHER REFERENCES.—On and after the
5 date of the enactment of this Act, any reference in
6 any other Federal law, Executive order, rule, regula-
7 tion, or delegation of authority to the “Director of
8 the Bureau of Citizenship and Immigration Serv-
9 ices” or the “Bureau of Citizenship and Immigration
10 Services” shall be deemed to be a reference to the
11 Director of United States Citizenship and Immigra-
12 tion Services or United States Citizenship and Immi-
13 gration Services, respectively.

14 (e) CLERICAL AMENDMENT.—The table of contents
15 in section 1(b) of such Act is amended by amending the
16 item relating to section 451 to read as follows:

“Sec. 451. United States Citizenship and Immigration Services.”.

17 (f) CONFORMING AMENDMENTS.—The Homeland Se-
18 curity Act of 2002 is amended—

19 (1) in subparagraph (E) of section 103(a) (6
20 U.S.C. 113(a)), by striking “A Director of the Bu-
21 reau of Citizenship and Immigration Services” and
22 inserting “A Director of United States Citizenship
23 and Immigration Services”;

24 (2) in section 452 (6 U.S.C. 272)—

1 (A) in paragraphs (1), (2), and (3) of sub-
2 section (b), by striking “the Bureau of Citizen-
3 ship and Immigration Services” each place it
4 appears and inserting “United States Citizen-
5 ship and Immigration Services”;

6 (B) in subsection (c)—

7 (i) in subparagraphs (A) and (E) of
8 paragraph (1), by striking “the Bureau of
9 Citizenship and Immigration Services”
10 each place it appears and inserting
11 “United States Citizenship and Immigra-
12 tion Services”; and

13 (ii) in paragraph (2), by striking “Di-
14 rector of the Bureau of Citizenship and
15 Immigration Services” and inserting “Di-
16 rector of United States Citizenship and
17 Immigration Services”;

18 (C) in subsection (d)—

19 (i) in paragraph (2), by striking “the
20 Bureau of Citizenship and Immigration
21 Services” and inserting “United States
22 Citizenship and Immigration Services”;
23 and

24 (ii) paragraph (4), by striking “Direc-
25 tor of the Bureau of Citizenship and Immi-

1 gration Services” and inserting “Director
2 of United States Citizenship and Immigra-
3 tion Services”;

4 (D) in paragraph (2) of subsection (e), by
5 striking “the Bureau of Citizenship and Immi-
6 gration Services” and inserting “United States
7 Citizenship and Immigration Services”;

8 (E) in subsection (f)—

9 (i) in the heading, by striking “BU-
10 REAU OF CITIZENSHIP AND IMMIGRATION
11 SERVICES” and inserting “UNITED
12 STATES CITIZENSHIP AND IMMIGRATION
13 SERVICES”; and

14 (ii) by striking “Director of the Bu-
15 reau of Citizenship and Immigration Serv-
16 ices” and inserting “Director of United
17 States Citizenship and Immigration Serv-
18 ices”; and

19 (F) in subsection (g)—

20 (i) in subparagraphs (B) and (D) of
21 paragraph (1), by striking “the Bureau of
22 Citizenship and Immigration Services”
23 each place it appears and inserting
24 “United States Citizenship and Immigra-
25 tion Services”; and

1 (ii) in paragraph (2), by striking “the
2 Bureau of Citizenship and Immigration
3 Services” each place it appears and insert-
4 ing “United States Citizenship and Immi-
5 gration Services”;

6 (3) in section 453 (6 U.S.C. 273)—

7 (A) in subsection (a)—

8 (i) in the matter preceding paragraph
9 (1), by striking “Director of the Bureau of
10 Citizenship and Immigration Services” and
11 inserting “Director of United States Citi-
12 zenship and Immigration Services”;

13 (ii) in paragraphs (1) and (3), by
14 striking “the Bureau of Citizenship and
15 Immigration Services” each place it ap-
16 pears and inserting “United States Citi-
17 zenship and Immigration Services”; and

18 (iii) in paragraph (2)—

19 (I) by striking “the Bureau of
20 Citizenship and Immigration Serv-
21 ices” and inserting “United States
22 Citizenship and Immigration Serv-
23 ices”; and

1 (II) by striking “such bureau”
2 and inserting “United States Citizen-
3 ship and Immigration Services”; and

4 (B) in subsection (b), in the matter pre-
5 ceding paragraph (1), by striking “Bureau of
6 Citizenship and Immigration Services” and in-
7 serting “United States Citizenship and Immi-
8 gration Services”;

9 (4) in section 456 (6 U.S.C. 275) by striking
10 “Director of the Bureau of Citizenship and Immi-
11 gration Services” each place it appears and inserting
12 “Director of United States Citizenship and Immigra-
13 tion Services”;

14 (5) in subparagraph (A) of section 462(b)(2) (6
15 U.S.C. 279(b)(2)), by striking “Director of the Bu-
16 reau of Citizenship and Immigration Services” and
17 inserting “Director of United States Citizenship and
18 Immigration Services”;

19 (6) in subsections (a), (b), and (d) of section
20 476 (6 U.S.C. 296), by striking “the Bureau of Citi-
21 zenship and Immigration Services” each place it ap-
22 pears and inserting “United States Citizenship and
23 Immigration Services”; and

24 (7) in section 478 (6 U.S.C. 298)—

25 (A) by striking subsection (b);

1 (B) by striking the following:

2 “(a) ANNUAL REPORT.—

3 “(1) IN GENERAL.—One year after”;

4 (C) by inserting the following:

5 “(a) IN GENERAL.—One year after”;

6 (D) by striking the following:

7 “(2) MATTER INCLUDED.—The report shall”;

8 (E) by inserting the following:

9 “(b) MATTER INCLUDED.—The report shall”;

10 (F) by redesignating subparagraphs (A)
11 through (H) as paragraphs (1) through (8), re-
12 spectively; and

13 (G) by striking “The Department of Jus-
14 tice” in new paragraph (5) and replacing it
15 with “The Department of Homeland Security”.

16 (g) REPEALS.—

17 (1) IN GENERAL.—The following provisions of
18 the Homeland Security Act of 2002 are repealed:

19 (A) Section 459 (6 U.S.C. 276).

20 (B) Section 460 (6 U.S.C. 277).

21 (C) Section 461 (6 U.S.C. 278).

22 (D) Section 472 (6 U.S.C. 292).

23 (E) Section 473 (6 U.S.C. 293).

24 (F) Section 474 (6 U.S.C. 294).

25 (G) Section 475 (6 U.S.C. 295).

1 (H) Section 477 (6 U.S.C. 297).

2 (2) CLERICAL AMENDMENTS.—The table of
3 contents in section 1(b) of the Homeland Security
4 Act of 2002 is amended by striking the items relat-
5 ing to the following sections:

6 (A) Section 459.

7 (B) Section 460.

8 (C) Section 461.

9 (D) Section 472.

10 (E) Section 473.

11 (F) Section 474.

12 (G) Section 475.

13 (H) Section 477.

14 (h) EMPLOYEE DISCIPLINE.—Section 454 of the
15 Homeland Security Act of 2002 (6 U.S.C. 274) is amend-
16 ed to read as follows:

17 **“SEC. 454. EMPLOYEE DISCIPLINE.**

18 “Notwithstanding any other provision of law, the Sec-
19 retary may impose disciplinary action on any employee of
20 United States Citizenship and Immigration Services who
21 knowingly deceives Congress or agency leadership on any
22 matter.”.

23 (i) COMBINATION PROHIBITION.—

1 (1) IN GENERAL.—Section 471 of the Home-
2 land Security Act of 2002 (6 U.S.C. 291) is amend-
3 ed to read as follows:

4 **“SEC. 471. COMBINATION PROHIBITION.**

5 “‘The authority provided by section 1502 may be used
6 to reorganize functions or organizational units within U.S.
7 Immigration and Customs Enforcement or United States
8 Citizenship and Immigration Services, but may not be
9 used to combine the two components into a single agency
10 or otherwise to combine, join, or consolidate functions or
11 organizational units of the two components with each
12 other.’”.

13 (2) CLERICAL AMENDMENT.—The table of con-
14 tents in section 1(b) of the Homeland Security Act
15 of 2002 is amended by amending the item relating
16 to section 471 to read as follows:

“Sec. 471. Combination prohibition.”.

17 **SEC. 427. FRAUD PREVENTION.**

18 (a) PROSPECTIVE ANALYTICS TECHNOLOGY.—

19 (1) PLAN FOR IMPLEMENTATION.—Not later
20 than 180 days after the date of the enactment of
21 this Act, the Secretary of Homeland Security shall
22 develop a plan to digitize the remaining paper bio-
23 metrics files of past immigration benefits applica-
24 tions and use advanced analytics software to ensure
25 the proactive detection of fraud in immigration bene-

1 fits applications and petitions and to ensure that
2 any such applicant or petitioner does not pose a
3 threat to national security.

4 (2) IMPLEMENTATION OF PLAN.—Not later
5 than one year after the date of the submission of the
6 plan under subsection (1), the Secretary of Home-
7 land Security shall begin implementation of the plan.

8 **SEC. 428. BORDER SECURITY AND TRADE MODERNIZATION**
9 **TRUST FUND.**

10 (a) BORDER SECURITY TRUST FUND.—Subtitle C of
11 title IV of the Homeland Security Act of 2002, as amend-
12 ed by this title, is further amended by adding at the end
13 the following new section:

14 **“SEC. 438. BORDER SECURITY AND TRADE MODERNIZATION**
15 **TRUST FUND.**

16 “(a) ESTABLISHMENT.—There is hereby established
17 in the Treasury of the United States a trust fund to be
18 known as the ‘Border Security and Trade Modernization
19 Trust Fund’ (in this section referred to as the ‘Fund’).

20 “(b) DEPOSITS TO THE FUND.—There shall be de-
21 posited in the Fund the following:

22 “(1) Amounts authorized and appropriated to
23 that Fund.

24 “(2) Surcharges established in subsection (f).

25 “(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

1 “(B) the Secretary of State shall charge a
2 surcharge of \$20 on the machine-readable visa
3 fee established under section 103 of the En-
4 hanced Border Security and Visa Entry Reform
5 Act of 2002 (8 U.S.C. 1713).

6 “(2) DEPOSIT OF SURCHARGES.—Surcharges
7 collected under this subsection shall be deposited in
8 the Fund established under this section.

9 “(g) ACCEPTANCE OF DONATIONS.—Notwith-
10 standing section 3113 of title 31, the Secretary of the
11 Treasury may accept for the Government a gift of money
12 for deposit in the Fund.

13 “(h) SUNSET.—Amounts may not be deposited in the
14 Fund and surcharges authorized under subsection (f) may
15 not be collected on the date that is the sooner of—

16 “(1) the date on which the Secretary notifies
17 the Committee on Homeland Security of the House
18 of Representatives and the Committee on Homeland
19 Security and Government Affairs of the Senate that
20 amounts deposited in the Fund exceed
21 \$35,000,000,000; or

22 “(2) 15 years after the first date on which
23 amounts are deposited in the Fund under subsection
24 (b).”.

1 (b) CLERICAL AMENDMENT.—The table of contents
2 in section 1(b) of the Homeland Security Act of 2002 is
3 amended by inserting after the item relating to section
4 437, as added by this title, the following new item:

“Sec. 438. Border security and trade modernization trust fund.”.

5 (c) CONFORMING AMENDMENT.—Notwithstanding
6 any other provision of law, penalties collected under sub-
7 chapter II of chapter 12 of title 8, United States Code,
8 shall be deposited in the Border Security and Trade Mod-
9 ernization Trust Fund established under section 438 of
10 the Homeland Security Act of 2002, as added by this sec-
11 tion.

12 (d) AUTHORIZATION OF APPROPRIATIONS.—There
13 are authorized to be appropriated to the Border Security
14 and Trade Modernization Trust Fund established under
15 section 438 of the Homeland Security Act of 2002, as
16 added by this section, \$4,500,000,000 for each of fiscal
17 years 2021 and 2022.

18 **SEC. 429. BORDER SECURITY IMPROVEMENT PLAN.**

19 (a) IN GENERAL.—Subtitle C of title IV of the
20 Homeland Security Act of 2002, as amended by this title,
21 is further amended by adding at the end the following:

22 **“SEC. 439. BORDER SECURITY IMPROVEMENT PLAN.**

23 “(a) IN GENERAL.—On the date the President sub-
24 mits to Congress a budget pursuant to section 1105 of
25 title 31, United States Code, the Secretary of Homeland

1 Security shall submit to the Committee on Homeland Se-
2 curity of the House of Representatives, the Committee on
3 Homeland Security and Governmental Affairs of the Sen-
4 ate, and the Comptroller General of the United States a
5 risk-based plan for improving security along the land bor-
6 ders of the United States.

7 “(b) TOPICS.—The plan required under subsection
8 (a) shall include a needs assessment and prioritization of
9 projects regarding the following:

10 “(1) Physical barriers, fencing, and tactical in-
11 frastructure.

12 “(2) Border Patrol mission-related technology
13 including cameras, sensors, anti-tunnel detection,
14 persistent surveillance and mobile and relocatable
15 technologies.

16 “(3) Border Patrol access to the border includ-
17 ing patrol roads and lighting.

18 “(4) Office of Field Operations mission-related
19 port of entry technology including non-intrusive in-
20 spection systems.

21 “(5) Office of Field Operations port of entry
22 and facility modernization.

23 “(6) Border Patrol interior checkpoint and fa-
24 cility 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.

1 “(5) A description of the methodology and anal-
2 yses used to inform the assessment conducted pursu-
3 ant to subparagraph (b) for deployment to particular
4 locations under the plan that includes the following:

5 “(A) Analyses of alternatives, where appro-
6 priate, including comparative costs and benefits.

7 “(B) An assessment of effects on relevant
8 government and non-non-government stake-
9 holders.

10 “(C) A description of other factors critical
11 to the decision-making process.

12 “(6) An identification of staffing requirements
13 under the plan, including full-time equivalents, con-
14 tractors, and detailed personnel, disaggregated by
15 activity.

16 “(7) A description of performance metrics for
17 the plan for assessing and reporting on the contribu-
18 tions of border security capabilities realized from
19 current and future investments.

20 “(8) A migrant surge response plan to improve
21 the Department of Homeland Security response rate
22 to future crises.

23 “(9) A description of the status of the actions
24 of the Department of Homeland Security to address
25 open recommendations by the Office of the Inspector

1 General of the Department and the Government Ac-
2 countability Office relating to border security, in-
3 cluding plans, schedules, and associated milestones
4 for fully addressing such recommendations.

5 “(10) A plan to consult State and local elected
6 officials on the eminent domain and construction
7 process relating to physical barriers (except that
8 such requirement may be satisfied through the sub-
9 mission of existing plans).

10 “(11) Certifications by the Under Secretary for
11 Management of the Department of Homeland Secu-
12 rity that—

13 “(A) the plan has been reviewed and ap-
14 proved in accordance with an acquisition review
15 management process that complies with capital
16 planning and investment control and review re-
17 quirements established by the Office of Manage-
18 ment and Budget, including as provided in Cir-
19 cular A-11, part 7; and

20 “(B) all activities under the plan comply
21 with Federal acquisition rules, requirements,
22 guidelines, and practices.

23 “(d) GAO EVALUATION.—Not later than 120 days
24 after receipt of the plan required under subsection (a) by
25 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

1 existing interagency task forces or centers within
2 such region, including the Border Enforcement Se-
3 curity Task Force established under section 443.

4 “(d) OPERATION.—After determining the regions in
5 which to establish IBET units under subsection (c)(2), the
6 Secretary may—

7 “(1) direct the assignment of Federal personnel
8 to such IBET units;

9 “(2) take other actions to assist Federal, State,
10 local, and Tribal entities to participate in such
11 IBET units, including providing financial assistance,
12 as appropriate, for operational, administrative, and
13 technological costs associated with such participa-
14 tion;

15 “(3) direct the development of policy and guid-
16 ance necessary to identify, assess, and integrate the
17 available partner resources in relevant border sector
18 security assessments and resource planning docu-
19 ments;

20 “(4) establish targets and performance meas-
21 ures for such IBET units; and

22 “(5) direct leadership of such IBET units to
23 monitor progress on such targets and performance
24 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;

1 “(3) identifies costs associated with IBET units
2 broken down by relevant categories designated at the
3 Secretary’s discretion;

4 “(4) identifies ways to support joint training
5 for IBET stakeholder agencies and radio interoper-
6 ability to allow for secure cross-border radio commu-
7 nications; and

8 “(5) identifies and assesses ways IBET, Border
9 Tunnel Task Forces, Border Enforcement Security
10 Task Forces, and the Integrated Cross-Border Mari-
11 time Law Enforcement Operation Program can bet-
12 ter align operations, including interdiction and inves-
13 tigation activities.”.

14 (b) CLERICAL AMENDMENT.—The table of contents
15 in section 1(b) of the Homeland Security Act of 2002 is
16 amended by inserting after the item relating to section
17 439, as added by this title, the following new item:

“Sec. 440. Integrated Border Enforcement Teams.”.

18 **SEC. 431. NO BAN ON INFORMATION SHARING.**

19 (a) IN GENERAL.—Subtitle C of title IV of the
20 Homeland Security Act of 2002, as amended by this title,
21 is further amended by adding at the end the following new
22 section:

23 **“SEC. 440A. ACCESS TO STATE, LOCAL, TRIBAL, AND TERRI-
24 TORIAL INFORMATION.**

25 “(a) AUTHORIZATION OF USE.—

1 “(1) IN GENERAL.—In the course of an inves-
2 tigation concerning a Federal crime within the juris-
3 diction of the Department, the Secretary may issue
4 in writing and cause to be served a subpoena requir-
5 ing the production of any biographical records,
6 State-issued identification information, driving
7 record information, vehicle registration information,
8 or criminal history information of a specific indi-
9 vidual from a State, local, Tribal, or territorial agen-
10 cy or department that the Secretary determines rel-
11 evant to such investigation, or requiring testimony
12 by the custodian of such materials to be produced
13 concerning the production and authenticity of such
14 materials.

15 “(2) CONTENTS.—A subpoena issued under
16 paragraph (1) shall describe the information de-
17 scribed in such paragraph required to be produced
18 and prescribe a return date within a reasonable pe-
19 riod of time within which such information can be
20 assembled and made available.

21 “(3) PRODUCTION OF RECORDS.—The produc-
22 tion of information under paragraph (1) may be re-
23 quired from any State, local, Tribal, or territorial
24 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

1 of the United States within the jurisdiction of which
2 the investigation described in subsection (a) is being
3 conducted or within the jurisdiction that the subject
4 of such investigation is located, to compel compli-
5 ance with such subpoena.

6 “(2) ORDER.—A court of the United States de-
7 scribed in paragraph (1) may issue an order requir-
8 ing the subpoenaed State agency or department, in
9 accordance with such subpoena, to appear, to
10 produce records, or to give testimony relating to the
11 matter under investigation. Any failure to obey the
12 order of the court may be punished by the court as
13 contempt thereof.

14 “(3) SERVICE OF PROCESS.—Any process under
15 this subsection may be served in any judicial district
16 in which the State, local, Tribal, or territorial agen-
17 cy or department may be found.

18 “(d) NONDISCLOSURE REQUIREMENT.—

19 “(1) IN GENERAL.—If the Secretary certifies
20 that otherwise there may result a danger to the na-
21 tional security of the United States, no person may
22 disclose to any other person that a subpoena was re-
23 ceived or information was provided pursuant to this
24 section, other than to—

1 “(A) those persons to whom such disclo-
2 sure is necessary in order to comply with such
3 subpoena;

4 “(B) an attorney to obtain legal advice
5 with respect to testimony or the production of
6 information in response to such subpoena; or

7 “(C) other persons as permitted by the
8 Secretary.

9 “(2) NOTICE OF NONDISCLOSURE REQUIRE-
10 MENT.—The subpoena, or an officer, employee, or
11 agency of the United States in writing, shall notify
12 the State, local, Tribal, or territorial agency or de-
13 partment to whom such subpoena is directed of the
14 nondisclosure requirements under paragraph (1).

15 “(3) FURTHER APPLICABILITY OF NONDISCLO-
16 SURE REQUIREMENTS.—Any person who receives a
17 disclosure under this subsection shall be subject to
18 the same prohibitions on disclosure described in
19 paragraph (1).

20 “(4) ENFORCEMENT OF NONDISCLOSURE RE-
21 QUIREMENT.—Whoever knowingly violates para-
22 graphs (1) or (3) shall be imprisoned for not more
23 than one year, and if such violation is committed
24 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

1 there is reason to believe that such nondisclosure re-
2 quirement is justified because otherwise there may
3 result a danger to the national security of the
4 United States.

5 “(3) REVIEW OF GOVERNMENT SUBMISSIONS.—
6 In all proceedings under this subsection, the court
7 shall review the submission of the Federal Govern-
8 ment, which may include classified information, ex
9 parte and in camera.

10 “(f) IMMUNITY FROM CIVIL LIABILITY.—Any State,
11 local, Tribal, or territorial agency or department, includ-
12 ing officers, agents, and employees of a non-natural per-
13 son, who in good faith produce the information requested
14 in a subpoena, shall not be liable in any court of the
15 United States to any customer or other person for such
16 production, or for nondisclosure of such production to the
17 customer or other person.

18 “(g) GUIDELINES.—The Secretary shall, by rule, es-
19 tablish such guidelines as are necessary to ensure the ef-
20 fective implementation of this section.

21 “(h) ANNUAL REPORTS.—The Secretary shall annu-
22 ally submit to the Committee on Homeland Security of
23 the House of Representatives and the Committee on
24 Homeland Security and Governmental Affairs of the Sen-
25 ate a report (which may include a classified annex but

1 with the presumption of declassification) on the use of
2 subpoenas under this subsection by the Secretary, which
3 shall include a discussion of—

4 “(1) the number of and reason for the sub-
5 poenas issued under this section by the Secretary
6 during the preceding year; and

7 “(2) a description of the outcome of each such
8 subpoena.”.

9 (b) CLERICAL AMENDMENT.—The table of contents
10 in section 1(b) of the Homeland Security Act of 2002 is
11 amended by inserting after the item relating to section
12 440, as added by this title, the following new item:

“Sec. 440A. Access to State, local, Tribal, and territorial information.”.

13 **SEC. 432. BORDER SECURITY ADVISORY COMMITTEE.**

14 (a) ESTABLISHMENT.—The Secretary of Homeland
15 Security shall establish a Border Security Advisory Com-
16 mittee (referred to in this section as the “Advisory Com-
17 mittee”).

18 (b) DUTIES.—

19 (1) IN GENERAL.—The Secretary of Homeland
20 Security shall consult the Advisory Committee, as
21 appropriate, on border security matters, including
22 the following:

23 (A) Verifying security claims and the bor-
24 der security metrics established by the Depart-
25 ment of Homeland Security under section 1092

1 of the National Defense Authorization Act for
2 Fiscal Year 2017 (Public Law 114–328; 6
3 U.S.C. 223).

4 (B) Developing, refining, and imple-
5 menting policies, programs, initiatives,
6 rulemakings, and security directives pertaining
7 to border security.

8 (2) RECOMMENDATIONS.—The Advisory Com-
9 mittee shall develop, at the request of the Secretary
10 of Homeland Security, recommendations for im-
11 provements to border security and may provide,
12 through the Secretary, recommendations to Con-
13 gress.

14 (c) MEMBERSHIP.—

15 (1) COMPOSITION.—The Advisory Committee
16 shall be composed of the following:

17 (A) Voting members appointed by the Sec-
18 retary.

19 (B) Nonvoting members, serving in an ad-
20 visory capacity, who shall be designated by—

21 (i) Customs and Border Protection;

22 (ii) Immigration and Customs En-
23 forcement;

24 (iii) the Coast Guard; and

1 (iv) such other Federal department or
2 agency as the Secretary considers appro-
3 priate.

4 (2) APPOINTMENT.—The Secretary of Home-
5 land Security shall appoint voting members from
6 among stakeholders including representatives from
7 the following:

8 (A) Labor organizations representing fed-
9 eral law enforcement personnel with border se-
10 curity as their primary mission;

11 (B) Relevant Federal, State, local, and
12 Tribal law enforcement, first responders, and
13 security experts with at least five years of bor-
14 der security operations or research experience
15 in a state that borders the northern, southern,
16 or coastal borders of the United States.

17 (C) Former officials of the Department of
18 Homeland Security with experience in border
19 security.

20 (D) Other groups as the Secretary con-
21 siders appropriate.

22 (3) CHAIRPERSON.—The Advisory Committee
23 shall select a chairperson from among its voting
24 members.

25 (4) TERM OF OFFICE.—

1 (A) IN GENERAL.—The term of each vot-
2 ing member of the Advisory Committee shall be
3 2 years, but a voting member may continue to
4 serve until the Secretary of Homeland Security
5 appoints a successor.

6 (B) REAPPOINTMENT.—A voting member
7 of the Advisory Committee may be reappointed.

8 (C) REMOVAL.—The Secretary of Home-
9 land Security may review the participation of a
10 member of the Advisory Committee and remove
11 such member for cause at any time.

12 (d) NONAPPLICABILITY OF FEDERAL ADVISORY
13 COMMITTEE ACT.—The Federal Advisory Committee Act
14 (5 U.S.C. App.) shall not apply to the Border Security
15 Advisory Committee.

16 **SEC. 433. BORDER TUNNEL DETECTION.**

17 (a) IN GENERAL.—Subtitle B of title IV of the
18 Homeland Security Act of 2002 (6 U.S.C. 211 et seq.),
19 as amended by this title, is further amended by adding
20 at the end the following new section:

21 **“SEC. 420C. BORDER TUNNEL TASK FORCES.**

22 “(a) ESTABLISHMENT.—There is established within
23 the Department a program to be known as the Border
24 Tunnel Task Force program (referred to in this section
25 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;

1 “(4) identifies ways to support joint training
2 for BTTF stakeholder agencies;

3 “(5) identifies and assesses ways BTTF, IBET,
4 and Border Enforcement Security Task Forces can
5 better align operations, including interdiction and in-
6 vestigation activities; and

7 “(6) identifies gaps in BTTF technological ca-
8 pability to detect cross-border tunnel threats.”.

9 (b) CLERICAL AMENDMENT.—The table of contents
10 in section 1(b) of the Homeland Security Act of 2002 is
11 amended by inserting after the item relating to section
12 420B, as added by this title, the following new item:

“Sec. 420C. Border Tunnel Task Forces.”.

13 **SEC. 434. SUBTERRANEAN OPERATIONS.**

14 (a) IN GENERAL.—Subtitle B of title IV of the
15 Homeland Security Act of 2002 (6 U.S.C. 211 et seq.),
16 as amended by this title, is further amended by adding
17 at the end the following new section:

18 **“SEC. 420D. NATIONAL SUBTERRANEAN OPERATIONS PRO-**
19 **GRAM.**

20 “(a) ESTABLISHMENT.—There is established within
21 U.S. Customs and Border Protection a program to known
22 as the ‘National Subterranean Operations Program’ (re-
23 ferred to in this section as ‘the program’). The program
24 shall be headed by an Assistant Chief, who shall be ap-
25 pointed 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

1 other relevant Federal entities as determined by
2 the Assistant Chief.

3 (B) Best practices for interdicting and re-
4 mediating illicit cross-border tunnels.

5 (C) Processes, in coordination with Home-
6 land Security Investigations and relevant Fed-
7 eral entities as determined by the Assistant
8 Chief, to request and share relevant illicit cross-
9 border tunnel location, operations, and technical
10 information.

11 (D) Indicators of specific types of illicit
12 cross-border tunnels found in each U.S. Border
13 Patrol sector to be periodically disseminated to
14 U.S. Border Patrol sector chiefs to educate
15 field personnel.

16 (E) A counter illicit cross-border tunnel
17 operations resource needs assessment that in-
18 cludes consideration of the following:

19 (i) Technology needs for conducting
20 counter illicit cross-border tunnel oper-
21 ations.

22 (ii) Staffing needs, including the fol-
23 lowing::

1 (I) A position description for
2 U.S. Border Patrol counter cross-bor-
3 der tunnel operations personnel.

4 (II) Specialized skills required of
5 counter cross-border tunnel operations
6 personnel.

7 (III) The number of full time
8 employees needed to conduct illicit
9 counter cross-border tunnel oper-
10 ations, disaggregated by U.S. Border
11 Patrol sector.

12 (IV) Training requirements for
13 identified staffing needs.

14 (2) REPORT TO CONGRESS.—Not later than one
15 year after the date of enactment of this Act, the
16 Commissioner of U.S. Customs and Border Protec-
17 tion shall submit to the Committee on Homeland Se-
18 curity of the House of Representatives and the Com-
19 mittee on Homeland Security and Governmental Af-
20 fairs of the Senate a report on the implementation
21 of subsection (b).

22 (c) CLERICAL AMENDMENT.—The table of contents
23 in section 1(b) of the Homeland Security Act of 2002 is
24 amended by inserting after the item relating to section
25 420C, as added by this title, the following new item

“Sec. 420D. National Subterranean Operations Program.”.

1 **SEC. 435. BORDER ENFORCEMENT SECURITY TASK FORCE**
2 **UPDATES.**

3 (a) UPDATED PURPOSE.—Subsection (b) of section
4 432 of the Homeland Security Act of 2002 (6 U.S.C. 240)
5 is amended—

6 (1) in paragraph (1), by striking “and” after
7 the semicolon at the end;

8 (2) in paragraph (2), by striking the period at
9 the end and inserting “; and”; and

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

12 “(3) detecting, investigating, preventing, and
13 responding to terrorism, transnational criminal orga-
14 nizations, and other violations of law related to bor-
15 der security.”.

16 (b) UPDATED CONSIDERATIONS FOR ESTABLISH-
17 MENT OF UNITS.—Paragraph (2) of section 432(c) of the
18 Homeland Security Act of 2002 (6 U.S.C. 240(c)) is
19 amended—

20 (1) in the matter preceding subparagraph (A)—

21 (A) in the first sentence, by striking “ju-
22 risdictions” and inserting “regions”;

23 (B) by striking “Before” and inserting
24 “When”; and

1 (C) by striking “shall consider” and insert-
2 ing “shall apply risk-based criteria that takes
3 into consideration”;

4 (2) in subparagraph (B), by inserting “and”
5 after the semicolon at the end; and

6 (3) by striking subparagraphs (C) and (D) and
7 inserting the following new subparagraph:

8 “(C) Whether, in accordance with para-
9 graph (3), other joint cross-border initiatives al-
10 ready take place within the region in which the
11 BEST unit would be established.”.

12 (e) UPDATED REPORT.—Subsection (e) of section
13 432 of the Homeland Security Act of 2002 (6 U.S.C. 240)
14 is amended to read as follows:

15 “(e) REPORTS.—Not later than 180 days after the
16 date of the enactment of this subsection and biannually
17 thereafter for the following six years, the Secretary shall
18 submit to the Committee on Homeland Security of the
19 House of Representatives and the Committee on Home-
20 land Security and Governmental Affairs of the Senate a
21 report that—

22 “(1) describes the effectiveness of BEST units
23 in fulfilling the purposes specified in subsection (b);

24 “(2) identifies challenges to the sustainment of
25 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 (1) in subsection (c)—

2 (A) in paragraph (1)(D), by inserting a
3 semicolon at the end; and

4 (B) in paragraph (3), by striking “jurisdic-
5 tion” each place it appears and inserting “re-
6 gion”; and

7 (2) in subsection (d), in the matter preceding
8 paragraph (1), by striking “jurisdictions” and in-
9 serting “regions”.

10 **SEC. 436. EXTENSION OF PORT OF ENTRY DONATION AU-**
11 **THORITY.**

12 Subparagraph (A) of section 482(b)(4) of the Home-
13 land Security Act of 2002 (6 U.S.C. 301a(b)(4)) is
14 amended by striking “4 years” and inserting “8 years”.

15 **TITLE V—TRANSPORTATION**
16 **SECURITY**

17 **SEC. 501. AUTHORIZATION OF APPROPRIATIONS FOR SALA-**
18 **RIES, OPERATION, AND MAINTENANCE OF**
19 **THE TRANSPORTATION SECURITY ADMINIS-**
20 **TRATION.**

21 Subsection (v) of section 114 of title 49, United
22 States Code, is amended—

23 (1) in paragraph (2), by striking “and” after
24 the semicolon at the end;

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

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

5 “(4) \$8,076,294,000 for fiscal year 2022.”.

6 **SEC. 502. RETENTION OF SECURITY SERVICE FEE BY THE**
7 **TRANSPORTATION SECURITY ADMINISTRA-**
8 **TION.**

9 (a) IN GENERAL.—Subsection (i) of section 44940 of
10 title 49, United States Code, is repealed.

11 (b) CONFORMING AMENDMENT.—Paragraph (3) of
12 section 44940(c) is amended by striking “Beginning on
13 October 1, 2027, fees” and inserting “Fees”.

14 **SEC. 503. EMERGING AND FUTURE THREATS TASK FORCE.**

15 (a) IN GENERAL.—Not later than 90 days after the
16 date of the enactment of this Act, the Administrator of
17 the Transportation Security Administration, in consulta-
18 tion with the Director of National Intelligence and the in-
19 telligence community (as such term is defined in section
20 3(4) of the National Security Act of 1947 (50 U.S.C.
21 3003(4))) and the heads of other Federal agencies, as de-
22 termined appropriate by the Administrator, shall establish
23 a task force to conduct an analysis of emerging and poten-
24 tial future threats to transportation security.

1 (b) MEMBERSHIP.—The task force established under
2 subsection (a) shall be comprised of employees of the De-
3 partment of Homeland Security who, in carrying out the
4 analysis required under such subsection, shall consult with
5 the Director of National Intelligence and the intelligence
6 community and the heads of Federal agencies, as deter-
7 mined appropriate by the Administrator.

8 (c) DEADLINE.—Not later than 270 days after the
9 Administrator establishes the task force under subsection
10 (a), the task force shall submit to the Administrator the
11 analysis required under such subsection.

12 (d) ELEMENTS.—The analysis required under sub-
13 section (a) shall include emerging and potential future
14 threats posed by the following:

15 (1) Evolving tactics by terrorist organizations
16 that may pose a catastrophic risk to an aviation or
17 surface transportation entity.

18 (2) Explosive and explosive devices or attacks
19 involving the use of explosives that may cause cata-
20 strophic damage to an aviation or surface transpor-
21 tation system.

22 (3) Chemical or biological agents being released
23 in either aviation or surface transportation systems.

1 (4) Cyberthreat actors seeking to undermine
2 confidence in transportation systems or cause service
3 disruptions that jeopardize transportation security.

4 (5) Unmanned aerial systems with the capa-
5 bility of inflicting harm on transportation targets.

6 (6) Individuals or groups seeking to attack soft
7 targets, public areas, or crowded spaces of transpor-
8 tation systems, including attacks against Transpor-
9 tation Security Administration employees and other
10 security personnel.

11 (7) Foreign actors seeking to exploit
12 vulnerabilities posed by the inconsistent or inad-
13 equate security screening protocols at last point of
14 departure airports with direct flights to the United
15 States.

16 (8) Information sharing challenges within the
17 Federal Government and among partner govern-
18 ments.

19 (9) Information sharing challenges between the
20 Administration or other relevant Federal agencies
21 and transportation stakeholders, including air car-
22 riers, airport operators, surface transportation oper-
23 ators, and State and local law enforcement.

24 (10) Growth in passenger volume in both the
25 aviation and surface transportation sectors.

1 (e) MITIGATION.—Not later than 120 days after the
2 completion of the analysis required under subsection (a),
3 the Administrator of the Transportation Security Admin-
4 istration shall develop, as appropriate, a threat mitigation
5 strategy for each of the threats examined in such analysis,
6 and—

7 (1) assign appropriate resources of the Admin-
8 istration to address such threats, based on cal-
9 culated risk; or

10 (2) provide recommendations through the De-
11 partment of Homeland Security to the appropriate
12 Federal department or agency responsible for ad-
13 dressing such threats.

14 (f) STAKEHOLDER ENGAGEMENT.—When carrying
15 out the analysis required under subsection (a), the Admin-
16 istrator of the Transportation Security Administration
17 shall engage transportation stakeholders referred to in
18 subsection (b)(9) and account for security concerns of
19 transportation operators by—

20 (1) convening not fewer than three industry day
21 events for such transportation stakeholders to hear
22 from relevant public and private sector security part-
23 ners and provide feedback on threats such transpor-
24 tation stakeholders identify as emerging;

1 (2) developing strategies to solicit feedback on
2 a consistent basis from such transportation stake-
3 holders across all modes of transportation and pro-
4 viding consistent responses to stakeholder concerns;

5 (3) improving the quality, timeliness, and rel-
6 evancy of information sharing products disseminated
7 by the Administration to such transportation stake-
8 holders, including classified information sharing
9 products;

10 (4) coordinating security incident response and
11 communications drills, including tabletop exercises,
12 to improve incident preparedness and response capa-
13 bilities across transportation modes and among
14 transportation systems;

15 (5) encouraging regular communication between
16 Federal Security Directors, Field Intelligence Offi-
17 cers, Federal Air Marshal Special Agents in Charge,
18 and such transportation stakeholders;

19 (6) establishing regular opportunities for senior
20 Administration leadership to engage with such trans-
21 portation stakeholders regarding changes in the
22 threat environment and how the Administration can
23 offer security support to address such changes; and

24 (7) briefing the Aviation Security Advisory
25 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

1 individual's enrollment in a trusted traveler program
2 being reinstated.

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

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

16 (4) The extent to which travelers are informed
17 about reconsideration procedures regarding enroll-
18 ment in a trusted traveler program.

19 **SEC. 505. ENROLLMENT REDRESS.**

20 Notwithstanding any other provision of law, the Sec-
21 retary of Homeland Security shall, with respect to an indi-
22 vidual whose enrollment in a trusted traveler program was
23 revoked in error extend by an amount of time equal to
24 the period of revocation the period of active enrollment

1 in such a program upon re-enrollment in such a program
2 by such an individual.

3 **SEC. 506. TRAINING REQUIRED.**

4 (a) IN GENERAL.—Not later than 1 year after the
5 date of the enactment of this Act, the Administrator of
6 the Transportation Security Administration shall develop
7 and implement training for frontline Administration per-
8 sonnel regarding the screening of pregnant women and
9 families with young children at passenger screening check-
10 points. Such training shall include the following:

11 (1) Information relating to concerns of preg-
12 nant women relating to the use of Advanced Imag-
13 ing Technology and appropriate opt-out procedures
14 and alternative screening procedures.

15 (2) Guidelines to assist pregnant women and
16 families traveling with young children effectively and
17 efficiently complete the screening process in a man-
18 ner that is respectful and improves the overall func-
19 tioning of the screening checkpoint.

20 (3) Communication and procedural guidelines
21 for frontline Administration personnel to assist with
22 passenger divestiture for pregnant women and fami-
23 lies traveling with young children to improve the ef-
24 fectiveness and overall passenger experience at the
25 screening checkpoint.

1 (b) COMMUNICATIONS STRATEGY.—In conjunction
2 with the implementation of the training required under
3 subsection (a), the Administrator of the Transportation
4 Security Administration shall develop and implement a
5 communications strategy for pregnant women and families
6 traveling with young children to inform such women and
7 families of the procedures and guidelines described in such
8 subsection, including providing information to relevant
9 passengers through social media, the Administration’s
10 public website, the Administration’s customer service call
11 center, and partnerships with aviation stakeholders, in-
12 cluding air carriers and airport operators.

13 (c) PASSENGER SUPPORT SPECIALISTS.—In carrying
14 out subsections (a) and (b), the Administrator of the
15 Transportation Security Administration shall, to the ex-
16 tent possible, make available passenger support specialists,
17 upon request, to pregnant women and families traveling
18 with young children to assist with screening checkpoint in-
19 formation, concerns, and procedures.

20 (d) TSA FAMILY LANES FEASIBILITY ASSESS-
21 MENT.—Not later than 180 days after the date of the en-
22 actment of this Act, the Administrator of the Transpor-
23 tation Security Administration shall conduct a feasibility
24 assessment to determine whether screening processes and
25 the screening experience may be improved for travelers by

1 developing optional, dedicated screening lanes for families
2 traveling with young children at airports where the check-
3 point configuration would allow and where the overall
4 functioning of the checkpoint would not be inhibited in
5 terms of passenger throughput or security effectiveness.

6 (e) BRIEFING TO CONGRESS.—Not later than 30
7 days after the implementation of the training required
8 under subsection (a), the Administrator of the Transpor-
9 tation Security Administration shall brief the Committee
10 on Homeland Security of the House of Representatives
11 and the Committee on Commerce, Science, and Transpor-
12 tation of the Senate on progress regarding the implemen-
13 tation of this Act and improvements made to the screening
14 process for pregnant women and families traveling with
15 young children.

16 **SEC. 507. IDENTITY AND TRAVEL DOCUMENT**
17 **VERIFICATION.**

18 Section 44901 of title 49, United States Code, is
19 amended by adding at the end the following new sub-
20 section:

21 “(m) ESTABLISHMENT OF SCREENING SYSTEM FOR
22 CERTAIN PERSONS.—Not later than December 31, 2020,
23 the Administrator of the Transportation Security Admin-
24 istration shall, subject to the availability of appropriations,
25 implement an identity and travel document verification

1 system designed to establish a secure, automated system
2 at all airports for verifying identity and travel documents
3 of persons seeking entry into the sterile area of an airport.

4 Such system shall—

5 “(1) assess the need for security screening per-
6 sonnel to perform identity and travel document
7 verification for such passengers, thereby assessing
8 the overall number of such screening personnel;

9 “(2) reduce the average wait time of such pas-
10 sengers;

11 “(3) reduce overall operating expenses of the
12 Administration;

13 “(4) be integrated with the Administration’s
14 watch list matching program; and

15 “(5) be integrated with other technologies to
16 further facilitate risk-based passenger screening at
17 checkpoints, to the extent practicable and consistent
18 with security standards.”.

19 **SEC. 508. STANDARD OPERATING PROCEDURES AT AIR-**
20 **PORT CHECKPOINTS.**

21 (a) STANDARDIZATION.—The Administrator of the
22 Transportation Security Administration shall require, to
23 the extent practicable, that standard operating procedures
24 at airport checkpoints for passengers and carry-on bag-

1 gage are carried out in a uniform manner among similarly
2 situated airports.

3 (b) REPORT TO CONGRESS.—Not later than 270 days
4 after the date of the enactment of this Act, the Adminis-
5 trator of the Transportation Security Administration shall
6 submit to the Committee on Homeland Security of the
7 House of Representatives and the Committee on Com-
8 merce, Science, and Transportation of the Senate a report
9 on how standard operating procedures were made uniform
10 in accordance with subsection (a).

11 (c) AUDITS.—Beginning one year after the date of
12 the enactment of this Act, the Inspector General of the
13 Department of Homeland Security shall conduct periodic
14 audits of adherence to the standard operating procedures,
15 as established by the Administrator of the Transportation
16 Security Administration, under this section of screening
17 personnel at large, medium, and small airports in diverse
18 geographical areas.

19 **SEC. 509. CANINE DETECTION RESEARCH AND DEVELOP-**
20 **MENT.**

21 (a) IN GENERAL.—The Secretary of Homeland Secu-
22 rity shall conduct an audit of all canine training programs
23 of the Department of Homeland Security and convene a
24 working group of representatives from all such programs
25 to make recommendations on possible efficiencies that

1 could be gained by integrating training standards and fa-
2 cilities.

3 (b) CANINE STAFFING ALLOCATION MODEL.—The
4 Administrator of the Transportation Security Administra-
5 tion shall develop a staffing allocation model for canines
6 to determine the optimal number of passenger screening
7 canines at airports in the United States.

8 (c) REPORT TO CONGRESS.—Not later than 180 days
9 after the date of the enactment of this Act, the Secretary
10 of Homeland Security shall submit to the Committee on
11 Homeland Security of the House of Representatives and
12 the Committee on Commerce, Science, and Transportation
13 of the Senate a report on the recommendations required
14 by subsection (a).

15 (d) BRIEFING TO CONGRESS.—

16 (1) IN GENERAL.—Not later than 180 days
17 after the date of the enactment of this Act, the Ad-
18 ministrator of the Transportation Security Adminis-
19 tration shall brief the Committee on Homeland Se-
20 curity of the House of Representatives and the Com-
21 mittee on Homeland Security and Governmental Af-
22 fairs and the Committee on Commerce, Science, and
23 Transportation of the Senate on the state of explo-
24 sives detection canine production and training in the
25 United States.

1 (2) CONTENTS.—The briefing required under
2 paragraph (1) shall include the following:

3 (A) An analysis of the steps the Transpor-
4 tation Security Administration may take to fos-
5 ter additional production of explosives detection
6 canines in the United States by the private sec-
7 tor.

8 (B) Perspectives from current explosives
9 detection canine industry stakeholders regard-
10 ing the impact of the Administration’s procure-
11 ment model on business considerations.

12 (C) An analysis regarding whether the Ad-
13 ministration effectively communicates canine
14 training guidelines and testing methodology to
15 the private sector.

16 (D) The extent to which physical capacity
17 limitations at current Administration-operated
18 sites hinder the operations of either the Admin-
19 istration or industry.

20 **SEC. 510. SECURITY INCIDENT RESPONSE AT AIRPORTS**
21 **AND SURFACE TRANSPORTATION HUBS.**

22 The Gerardo Hernandez Airport Security Act of 2015
23 (Public Law 114–50; 49 U.S.C. 44903 note) is amend-
24 ed—

25 (1) in section 3—

1 (A) in subsection (b), in the matter pre-
2 ceding paragraph (1), by striking “may” each
3 place it appears and inserting “shall”;

4 (B) by redesignating subsection (c) as sub-
5 section (d); and

6 (C) by inserting after subsection (b) the
7 following new subsection:

8 “(c) REVIEW.—The Administrator of the Transpor-
9 tation Security Administration shall review the active
10 shooter response guidelines specified for Department of
11 Homeland Security personnel under this section and make
12 a recommendation to the Secretary of Homeland Security
13 to modify such guidelines for personnel who are certified
14 Federal law enforcement officials and for personnel who
15 are uniformed but unarmed security officials.”; and

16 (2) in section 7—

17 (A) in subsection (b), in the matter pre-
18 ceding paragraph (1), by striking “may” each
19 place it appears and inserting “shall”;

20 (B) by redesignating subsections (c) and
21 (d) as subsections (d) and (e), respectively; and

22 (C) by inserting after subsection (b) the
23 following new subsection:

24 “(c) REVIEW.—The Administrator of the Transpor-
25 tation Security Administration shall review the active

1 shooter response guidelines specified for Department of
2 Homeland Security personnel under this section and make
3 a recommendation to the Secretary of Homeland Security
4 to modify such guidelines for personnel who are certified
5 Federal law enforcement officials and for personnel who
6 are uniformed but unarmed security officials.”.

7 **SEC. 511. ALTERNATE NEW SECURITY SCREENING PER-**
8 **SONNEL TRAINING PROGRAM COST AND FEA-**
9 **SIBILITY STUDY.**

10 Not later than 180 days after the date of the enact-
11 ment of this Act, the Administrator of the Transportation
12 Security Administration shall conduct a cost and feasi-
13 bility study of developing a training program for security
14 screening personnel that will provide such personnel with
15 an equal level of training as is provided in the training
16 program for new security screening personnel located at
17 the Federal Law Enforcement Training Center in Glynco,
18 Georgia, that could be conducted at or within 50 miles
19 of such security screening personnel’s duty station. Such
20 study should examine the use of online seminar and train-
21 ing platforms for portions of the training curriculum that
22 are conducive to such an outcome.

1 **SEC. 512. PROHIBITION OF ADVANCE NOTICE OF COVERT**
2 **TESTING TO SECURITY SCREENERS.**

3 Section 44935 of title 49, United States Code, is
4 amended by adding at the end the following new sub-
5 section:

6 “(m) PROHIBITION OF ADVANCE NOTICE TO SECUR-
7 RITY SCREENERS OF COVERT TESTING AND EVALUA-
8 TION.—

9 “(1) IN GENERAL.—The Administrator of the
10 Transportation Security Administration shall ensure,
11 to the greatest extent practicable, that information
12 concerning a covert test of a transportation security
13 system to be conducted by a covert testing office, the
14 Inspector General of the Department of Homeland
15 Security, or the Government Accountability Office is
16 not provided to any individual involved in such test
17 prior to the completion of such test.

18 “(2) EXCEPTIONS.—Notwithstanding para-
19 graph (1)—

20 “(A) an authorized individual involved in a
21 covert test of a transportation security system
22 may provide information concerning such covert
23 test to—

24 “(i) employees, officers, and contrac-
25 tors of the Federal Government (including
26 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

1 transportation security system for a covert test-
2 ing office is accompanied at the site of such test
3 by a cover team composed of one or more em-
4 ployees of such covert testing office for the pur-
5 pose of monitoring such test and confirming the
6 identity of personnel involved in such test under
7 subparagraph (B).

8 “(B) RESPONSIBILITY OF COVER TEAM.—
9 Under this paragraph, a cover team for a covert
10 test of a transportation security system shall—

11 “(i) monitor such test; and

12 “(ii) for the purpose of ensuring the
13 security of any individual in the vicinity of
14 a site at which such test is being con-
15 ducted, confirm, notwithstanding para-
16 graph (1), the identity of any individual
17 conducting such test to any appropriate in-
18 dividual if a security screener or other in-
19 dividual who is not a covered employee
20 identifies the individual conducting such
21 test as a potential threat.

22 “(C) AVIATION SCREENING.—Notwith-
23 standing subparagraph (A), the Transportation
24 Security Administration is not required to have
25 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,

1 means any individual who the individual
2 conducting such test determines needs to
3 know his or her status as an individual
4 conducting such test; or

5 “(ii) a covert test under paragraph
6 (3)(B)(i), means any individual who the
7 cover team monitoring such test deter-
8 mines needs to know the identity of such
9 cover team.

10 “(B) COVERED EMPLOYEE.—The term
11 ‘covered employee’ means any individual who
12 receives notice of a covert test before the com-
13 pletion of a test under paragraph (2)(B).

14 “(C) COVERT TEST.—

15 “(i) IN GENERAL.—The term ‘covert
16 test’ means an exercise or activity con-
17 ducted by a covert testing office, the In-
18 spector General of the Department of
19 Homeland Security, or the Government Ac-
20 countability Office to intentionally test,
21 compromise, or circumvent transportation
22 security systems to identify vulnerabilities
23 in such systems.

24 “(ii) LIMITATION.—Notwithstanding
25 clause (i), the term ‘covert test’ does not

1 mean an exercise or activity by an em-
2 ployee or contractor of the Transportation
3 Security Administration to test or assess
4 compliance with relevant regulations.

5 “(D) COVERT TESTING OFFICE.—The term
6 ‘covert testing office’ means any office of the
7 Transportation Security Administration des-
8 igned by the Administrator of the Transpor-
9 tation Security Administration to conduct cov-
10 ert tests of transportation security systems.

11 “(E) EMPLOYEE OF A COVERT TESTING
12 OFFICE.—The term ‘employee of a covert test-
13 ing office’ means an individual who is an em-
14 ployee of a covert testing office or a contractor
15 or an employee of a contractor of a covert test-
16 ing office.”.

17 **SEC. 513. EXPLOSIVE DETECTION TECHNOLOGY.**

18 The Secretary of Homeland Security shall prioritize
19 the research and facilitation of next generation tech-
20 nologies to detect explosives in the Nation’s surface trans-
21 portation systems.

1 **SEC. 514. RECURRENT VETTING FOR SURFACE TRANSPOR-**
2 **TATION CREDENTIAL-HOLDERS.**

3 Section 70105 of title 46, United States Code, is
4 amended by adding at the end the following new sub-
5 section:

6 “(r) RECURRENT VETTING.—

7 “(1) IN GENERAL.—Not later than 180 days
8 after the date of the enactment of this subsection,
9 the Secretary shall develop and implement a plan to
10 utilize the Federal Bureau of Investigation’s Rap
11 Back Service in order to establish recurrent vetting
12 capabilities for individuals holding valid transpor-
13 tation security cards under this section.

14 “(2) EXEMPTION.—Individuals holding valid
15 transportation security cards under this section who
16 are subject to recurrent vetting under the plan to
17 utilize the Rap Back Service referred to in para-
18 graph (1) shall be exempt from any recurrent deter-
19 minations or background checks under this section
20 to which such individuals would otherwise be subject
21 every five years in the absence of such utilization.”.

22 **SEC. 515. BIOMETRICS FOR TSA PRECHECK.**

23 (a) IN GENERAL.—Not later than September 30,
24 2023, the Administrator of the Transportation Security
25 Administration shall begin the utilization of biometrics to
26 verify the identity of travelers enrolled in the Administra-

1 tion's trusted traveler program, known as TSA PreCheck,
2 at security screening checkpoints in a manner which—

3 (1) protects the privacy and civil liberties of the
4 traveling public;

5 (2) improves the security and functionality of
6 the security screening checkpoint;

7 (3) leverages, to the extent practicable, existing
8 biometric repositories of the Department of Home-
9 land Security; and

10 (4) utilizes best available biometric technology
11 and algorithms to reduce instances of
12 misidentification.

13 (b) **WORKING GROUP ESTABLISHED.**—Not later than
14 30 days after the date of the enactment of this Act, the
15 Administrator of the Transportation Security Administra-
16 tion shall establish a working group comprised of relevant
17 transportation security stakeholders and any personnel de-
18 termined necessary by the Administrator to inform and
19 make recommendations for the successful implementation
20 of a biometrics identity process.

21 (c) **REPORT TO CONGRESS.**—Not later than one year
22 after the date of the enactment of this Act and annually
23 thereafter through 2023, the Administrator of the Trans-
24 portation Security Administration shall report to the Com-
25 mittee on Homeland Security of the House of Representa-

1 tives and the Committee on Commerce, Space, and Trans-
2 portation of the Senate on the status of the Administra-
3 tion's biometrics program.

4 **SEC. 516. SECURE FLIGHT PROGRAM.**

5 (a) IN GENERAL.—Not later than 180 days after the
6 date of the enactment of this Act, the Administrator of
7 the Transportation Security Administration shall ensure
8 that security screening checkpoints have real-time
9 connectivity to the Administration's Secure Flight vetting
10 system.

11 (b) SECURE FLIGHT REVIEW.—Not later than 1 year
12 after the date of the enactment of this Act, the Adminis-
13 trator of the Transportation Security Administration shall
14 develop and implement a plan to improve the capabilities
15 of the Administration's Secure Flight program, includ-
16 ing—

17 (1) improving coordination between Secure
18 Flight and air carriers;

19 (2) reducing screening errors resulting from in-
20 accurate or delayed Secure Flight data; and

21 (3) identifying additional resources needed to
22 upgrade information technology systems of Secure
23 Flight.

1 **SEC. 517. KNOWN CREW MEMBER PROGRAM.**

2 (a) IN GENERAL.—Not later than 180 days after the
3 enactment of this Act, the Administrator of the Transpor-
4 tation Security Administration shall implement new secu-
5 rity standards for the Administration’s Known Crew Mem-
6 ber program, including—

7 (1) updated standards for verifying crew iden-
8 tity at Known Crew Member-enabled checkpoints;
9 and

10 (2) cybersecurity standards for the Known
11 Crew Member program.

12 (b) COORDINATION.—In carrying out the require-
13 ments of subsection (a), the Administrator of the Trans-
14 portation Security Administration shall coordinate with
15 relevant transportation security stakeholders, including air
16 carriers and labor organizations representing pilots and
17 flight attendants.

18 **SEC. 518. SCREENING PARTNERSHIP PROGRAM.**

19 (a) IN GENERAL.—The Administrator of the Trans-
20 portation Security Administration shall promote and en-
21 courage airport participation in the Administration’s
22 Screening Partnership Program.

23 (b) BLUE RIBBON PANEL.—Not later than 90 days
24 after the date of the enactment of this Act, the Adminis-
25 trator of the Transportation Security Administration shall
26 convene a Blue Ribbon Panel to examine ways in which

1 the Screening Partnership Program can be improved, in-
2 cluding—

3 (1) allowing greater input for airport terminal
4 owners and operators into selecting a screening ven-
5 dor;

6 (2) reducing costs to the taxpayer by expanding
7 the Screening Partnership Program; and

8 (3) examining security screening programs of
9 foreign partners to outline best practices for public
10 private partnership for passenger screening.

11 **SEC. 519. HEADQUARTERS EFFICIENCY.**

12 Not later than 1 year after the date of the enactment
13 of this Act, the Administrator of the Transportation Secu-
14 rity Administration shall seek to reduce by 50 percent ad-
15 ministrative support contract costs for headquarters per-
16 sonnel.

17 **SEC. 520. REPEAL OF REGULATIONS.**

18 Sections 1408, 1517, and 1534 of the Implementing
19 Recommendations of the 9/11 Commission Act of 2007
20 are repealed.

21 **SEC. 521. SENSITIVE SECURITY INFORMATION.**

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

1 (1) ensure clear and consistent designation of
2 “Sensitive Security Information”, including reason-
3 able security justifications for so designating docu-
4 ments as such;

5 (2) develop and implement a schedule to regu-
6 larly review and update, as necessary, TSA Sensitive
7 Security Information Identification guidelines;

8 (3) develop a tracking mechanism for all Sen-
9 sitive Security Information redaction and designa-
10 tion challenges;

11 (4) document justifications for changes in posi-
12 tion regarding Sensitive Security Information
13 redactions and designations, and make such changes
14 accessible to TSA personnel for use with relevant
15 stakeholders, including air carriers, airport opera-
16 tors, surface transportation operators, and State and
17 local law enforcement, as necessary; and

18 (5) ensure that TSA personnel are adequately
19 trained on appropriate designation policies.

20 (b) **STAKEHOLDER OUTREACH.**—Not later than 180
21 days after the date of the enactment of this Act, the Ad-
22 ministratoꝛ of the Transportation Security Administration
23 (TSA) shall conduct outreach to relevant stakeholders de-
24 scribed in subsection (a)(4) that regularly are granted ac-
25 cess to Sensitive Security Information to raise awareness

1 of the TSA's policies and guidelines governing the classi-
2 fication and use of Sensitive Security Information.

3 **SEC. 522. INTERNATIONAL AVIATION SECURITY.**

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

9 (1) ensure the inclusion, as appropriate, of air
10 carriers and other transportation security
11 stakeholders in the development and implementa-
12 tion of security directives and emergency amend-
13 ments;

14 (2) document input provided by air carriers and
15 other transportation security stakeholders during the
16 security directive and emergency amendment devel-
17 opment and implementation processes;

18 (3) define, with the inclusion of feedback from
19 air carriers and other transportation security stake-
20 holders, a process, including time frames, for cancel-
21 ling or incorporating security directives and emer-
22 gency amendments into security programs;

23 (4) conduct engagement with foreign partners
24 on the implementation of security directives and
25 emergency amendments, as appropriate, including

1 recognition if existing security measures at a last
2 point of departure airport are found to provide com-
3 mensurate security as intended by potential new se-
4 curity directives and emergency amendments; and

5 (5) ensure that new security directives and
6 emergency amendments are focused on defined secu-
7 rity outcomes.

8 (b) BRIEFING TO CONGRESS.—Not later than 90
9 days after the date of the enactment of this Act, the Ad-
10 ministrator of the Transportation Security Administration
11 shall brief the Committee on Homeland Security of the
12 House of Representatives and the Committee on Com-
13 merce, Space, and Transportation of the Senate on the
14 guidelines described in this section.

15 (c) DECISIONS NOT SUBJECT TO JUDICIAL RE-
16 VIEW.—Notwithstanding any other provision of law, any
17 action of the Administrator of the Transportation Security
18 Administration under subsection (a) is not subject to judi-
19 cial review.

20 **SEC. 523. OFFICE OF INSPECTION ACCOUNTABILITY.**

21 (a) IN GENERAL.—The Administrator of the Trans-
22 portation Security Administration shall strengthen inter-
23 nal controls related to documentation accuracy of the Of-
24 fice of Inspection of the Administration by developing and
25 implementing—

1 (1) updates to criminal investigators' perform-
2 ance plans to reflect timely and accurate timesheet
3 submission;

4 (2) guidance and expectation for supervisory bi-
5 weekly timesheet review; and

6 (3) a formal plan for reviewing user access, not
7 less than annually, to ensure appropriate system ac-
8 cess and permission levels.

9 (b) INFORMATION SYSTEMS.—The Administrator of
10 the Transportation Security Administration shall work to
11 establish systems to assist the Office of Inspection of the
12 Administration with timesheet submission and approval
13 processes and improve data transfer and communication
14 between the timekeeping system and the Case Manage-
15 ment System.

16 (c) PREMIUM PAY ELIGIBILITY.—The Administrator
17 of the Transportation Security Administration shall de-
18 velop, formalize, and implement processes to ensure com-
19 pliance with relevant policies requiring criminal investiga-
20 tors and supervisors annually complete documentation cer-
21 tifying availability for Law Enforcement Availability Pay.

22 (d) RESOURCE ALLOCATION.—The Administrator of
23 the Transportation Security Administration shall develop
24 and implement guidance to ensure proper review of annual

1 calculations for resource allocation within the Office of In-
2 spection of the Administration.

3 **SEC. 524. CHECKPOINTS OF THE FUTURE.**

4 (a) IN GENERAL.—The Administrator of the Trans-
5 portation Security Administration shall develop passenger
6 self-screening solutions for PreCheck passengers in a man-
7 ner which—

8 (1) does not reduce the overall security posture
9 of the checkpoint; and

10 (2) improves the efficiency and overall effective-
11 ness of the checkpoint.

12 (b) REPORT TO CONGRESS.—Not later than 180 days
13 after the enactment of this Act and annually thereafter
14 for 5 years, the Administrator of the Transportation Secu-
15 rity Administration shall submit to the Committee on
16 Homeland Security of the House of Representatives and
17 the Committee on Commerce, Space, and Transportation
18 of the Senate a report on the status of the requirements
19 described in subsection (a).

20 **SEC. 525. AIR CARGO SECURITY.**

21 Not later than one year after the date of the enact-
22 ment of this Act the Inspector General for the Department
23 of Homeland Security shall conduct an audit of the Air
24 Cargo Division of the Transportation Security Adminis-
25 tration of the Department. This audit shall include—

1 (1) a review of resource and staffing allocations
2 for the Air Cargo Division;

3 (2) an examination of how the Air Cargo Divi-
4 sion's effectiveness in managing the Certified Cargo
5 Screening Program and Known Shipper Program;
6 and

7 (3) how effectively the Air Cargo Division
8 works collaboratively with U.S. Customs and Border
9 Protection to target high-risk cargo.

10 **SEC. 526. CHILDCARE.**

11 (a) IN GENERAL.—Not later than 30 days after the
12 date of the enactment of this Act, the Administrator of
13 the Transportation Security Administration shall convene
14 a working group comprised of personnel determined ap-
15 propriate by the Administrator to develop—

16 (1) recommendations for establishing childcare
17 facilities for employees at the Administration's head-
18 quarters facility;

19 (2) recommendations for establishing a facility
20 or otherwise assisting with childcare options for em-
21 ployees at airports; and

22 (3) options for the Administration to improve
23 flexibility for employees with children in need of
24 care.

1 (b) REPORT TO CONGRESS.—Not later than 1 year
2 after the date of the enactment of this Act, the Adminis-
3 trator of the Transportation Security Administration shall
4 submit to the Committee on Homeland Security of the
5 House of Representatives and the Committee on Com-
6 merce, Space, and Technology of the Senate a report on
7 the recommendations and findings of the working group
8 established in subsection (a).

9 **SEC. 527. PASSENGERS WITH PHYSICAL OR COGNITIVE DIS-**
10 **ABILITIES.**

11 Not later than one year after the date of the enact-
12 ment of this Act, the Administrator of the Transportation
13 Security Administration shall convene an event at each
14 airport at which the Administration conducts security
15 screening to increase awareness, understanding of screen-
16 ing protocols, and efficiency of the passenger screening ex-
17 perience for passengers with physical or cognitive disabil-
18 ities.

19 **SEC. 528. TSA HUMAN CAPITAL STRATEGIC PLAN.**

20 (a) HUMAN CAPITAL STRATEGIC PLAN DEFINED.—
21 In this section, the term “human capital strategic plan”
22 means a plan to evaluate and implement strategies for the
23 Transportation Security Administration’s selecting, devel-
24 oping, training, and managing a high-quality, productive
25 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.”.

1 **SEC. 529. SCREENING TECHNOLOGY DEPLOYMENT.**

2 (a) IN GENERAL.—Not later than 180 days after the
3 date of the enactment of this Act, the Administrator of
4 the Transportation Security Administration shall imple-
5 ment a policy to produce deployment plans for screening
6 technology. Such plans should—

7 (1) include airport risk assessments and all rel-
8 evant risk factors;

9 (2) consider relative airport risk when deter-
10 mining deployment order;

11 (3) provide rationale for deployment decisions,
12 including any specific risk factors considered;

13 (4) include a strategy for deployment to small
14 and medium airports to ensure consistency of secu-
15 rity operations across airports of all sizes; and

16 (5) include procurement strategy for each
17 screening technology to be deployed.

18 (b) CONTINUOUS EVALUATION OF DEPLOYED
19 EQUIPMENT.—Not later than 180 days after the date of
20 the enactment of this Act, the Administrator of the Trans-
21 portation Security Administration shall develop a strategy
22 for continuous evaluation of deployed screening tech-
23 nology. In developing such strategy, the Administrator
24 shall consider the following:

25 (1) The effectiveness of screening during the
26 lifespan of screening technology.

1 (2) How maintenance contracts for procured
2 screening technology can support the Administra-
3 tion's efforts to ensure continued effectiveness after
4 deployment of such technology.

5 (3) Periodic testing for the effectiveness of de-
6 ployed screening technology based on relative risk.

7 (c) AUDITS.—Beginning one year after the date of
8 the enactment of this Act, the Inspector General of the
9 Department of Homeland Security shall conduct an audit
10 of the Transportation Security Administration's efforts to
11 develop and implement deployment plans for screening
12 technology. Such audit shall determine if—

13 (1) the Administration has effectively produced
14 risk-based deployment plans for screening tech-
15 nologies;

16 (2) the screening technology deployment ad-
17 hered to deployment plans; and

18 (3) the deployment rate of screening tech-
19 nologies by type across airport size and geographical
20 areas.

21 (d) BRIEFING TO CONGRESS.—Not later than 270
22 days after the date of the enactment of this Act, the Ad-
23 ministrator of the Transportation Security Administration
24 shall brief the Committee on Homeland Security of the
25 House of Representatives and the Committee on Com-

1 merce, Science, and Transportation of the Senate on the
2 requirements described in this section.

3 **SEC. 530. REVIEW OF AVIATION SECURITY STAKEHOLDER**
4 **ACCESS TO HOMELAND SECURITY INFORMA-**
5 **TION NETWORK.**

6 The Secretary of Homeland Security, in coordination
7 with the Under Secretary for Intelligence and Analysis of
8 the Department of Homeland Security, shall review access
9 to the Homeland Security Information Network to deter-
10 mine if access by aviation security stakeholders in addition
11 to such stakeholders who already as of the date of the
12 enactment of this Act already have such access would ben-
13 efit aviation security.

14 **SEC. 531. AIRPORT PUBLIC AREA SECURITY ENHANCE-**
15 **MENT.**

16 (a) AIRPORT PUBLIC AREA SECURITY WORKING
17 GROUP ENGAGEMENT PLAN.—

18 (1) IN GENERAL.—Not later than one year
19 after the date of the enactment of this Act, the Ad-
20 ministrator of the Transportation Security Adminis-
21 tration (TSA) shall implement a plan to enhance
22 TSA engagement with the public area security work-
23 ing group established in accordance with section
24 1931 of the FAA Reauthorization Act of 2018 (49
25 U.S.C. 114 note; Public Law 115–254). Such plan

1 shall include descriptions of roles and responsibilities
2 for group members, mechanisms for collaboration,
3 and determinations regarding the frequency of work-
4 ing group meetings.

5 (2) BRIEFING TO CONGRESS.—Not later than
6 30 days after implementation of the plan required
7 under paragraph (1) is complete, the Administrator
8 shall brief the appropriate committees of Congress
9 on the details of such plan.

10 (b) SURVEY OF AIRPORT PUBLIC AREA SECURITY
11 EFFORTS.—

12 (1) IN GENERAL.—Not later than 180 days
13 after the date of the enactment of this Act, the Ad-
14 ministrator shall begin conducting a survey of public
15 and private stakeholders responsible for securing air-
16 port public areas to assess the following:

17 (A) The number of airport operations cen-
18 ters.

19 (B) The activities in which such airport
20 operations centers regularly engage.

21 (C) The stakeholders involved in such air-
22 port operations centers, including information
23 relating to staffing and participation of such
24 stakeholders.

1 (D) Availability of resources for such air-
2 port operations centers.

3 (E) Technology used to monitor and secure
4 airport public areas.

5 (F) Interoperability or other challenges as-
6 sociated with communication or other informa-
7 tion technology systems supporting such airport
8 operations centers.

9 (G) Policies and best practices used to pro-
10 vide situational awareness and coordinate air-
11 port public area security efforts.

12 (2) BRIEFING TO CONGRESS.—Not later than
13 30 days after completion of the survey required
14 under subsection (1), the Administrator shall brief
15 the appropriate committees of Congress a report on
16 the findings of such survey.

17 (c) TSA SUPPORT OF AIRPORT OPERATIONS CEN-
18 TERS.—

19 (1) IN GENERAL.—Not later than 90 days after
20 the briefing required under subsection (b)(2) and
21 not less frequently than once every five years there-
22 after, the Administrator shall develop and update,
23 respectively, a strategy for Administration engage-
24 ment with airport operations centers. Such strategy
25 shall—

1 (A) include specific goals and objectives for
2 the support of such airport operations centers
3 managed by public and private stakeholders re-
4 sponsible for securing airport public areas; and

5 (B) detail means of support—

6 (i) to direct deployment of Adminis-
7 tration personnel to such airport oper-
8 ations centers;

9 (ii) to provide to such stakeholders, as
10 appropriate, access to Department unclas-
11 sified or classified information sharing sys-
12 tems, including the Homeland Security In-
13 formation Network and Homeland Security
14 Data Network; and

15 (iii) for any activities determined ap-
16 propriate by the Administrator.

17 (2) BRIEFING TO CONGRESS.—Not later than
18 30 days after the strategy under subsection (1) is
19 complete, the Administrator shall brief the appro-
20 priate committees of Congress on the implementa-
21 tion of such strategy.

22 (d) DEFINITIONS.—In this section:

23 (1) ADMINISTRATION; TSA.—The terms “Ad-
24 ministration” and “TSA” mean the Transportation
25 Security Administration.

1 (2) ADMINISTRATOR.—The term “Adminis-
2 trator” means the Administrator of the Administra-
3 tion.

4 (3) APPROPRIATE COMMITTEES OF CON-
5 GRESS.—The term “appropriate committees of Con-
6 gress” means the Committee on Homeland Security
7 of the House of Representatives and the Committee
8 on Commerce, Science, and Transportation of the
9 Senate.

10 (4) DEPARTMENT.—The term “Department”
11 means the Department of Homeland Security.

12 (5) OPERATIONS CENTER.—The term “oper-
13 ations center” means a integrated and unified oper-
14 ation center established at a transportation facility
15 based on the framework made available to public
16 and private stakeholders pursuant to section 1987 of
17 the FAA Reauthorization Act of 2018 (49 U.S.C.
18 114 note; Public Law 115–254).

19 (6) PUBLIC AND PRIVATE STAKEHOLDERS.—
20 The term “public and private stakeholders” has the
21 meaning given such term in section 114(t)(1)(C) of
22 title 49, United States Code.

1 **TITLE VI—EMERGENCY PRE-**
2 **PAREDNESS, RESPONSE, AND**
3 **RECOVERY**

4 **Subtitle A—Grants, Training,**
5 **Exercises, and Coordination**

6 **SEC. 601. URBAN AREA SECURITY INITIATIVE.**

7 Section 2003 of the Homeland Security Act of 2002
8 (6 U.S.C. 604) is amended—

9 (1) in subsection (b)(2)(A), in the matter pre-
10 ceding clause (i), by inserting “, using the most up-
11 to-date data available,” after “assessment”;

12 (2) in subsection (d)(2), by amending subpara-
13 graph (B) to read as follows:

14 “(B) FUNDS RETAINED.—To ensure trans-
15 parency and avoid duplication, a State shall
16 provide each relevant high-risk urban area with
17 a detailed accounting of the items, services, or
18 activities on which any funds retained by the
19 State under subparagraph (A) are to be ex-
20 pended. Such accounting shall be provided not
21 later than 90 days after the date of which such
22 funds are retained.”; and

23 (3) by striking subsection (e) and inserting the
24 following new subsections:

1 “(e) THREAT AND HAZARD IDENTIFICATION RISK
2 ASSESSMENT AND CAPABILITY ASSESSMENT.—As a con-
3 dition of receiving a grant under this section, each high-
4 risk urban area shall submit to the Administrator a threat
5 and hazard identification and risk assessment and capa-
6 bility assessment—

7 “(1) at such time and in such form as is re-
8 quired by the Administrator; and

9 “(2) consistent with the Federal Emergency
10 Management Agency’s Comprehensive Preparedness
11 Guide 201, Second Edition, or such successor docu-
12 ment or guidance as is issued by the Administrator.

13 “(f) PERIOD OF PERFORMANCE.—The Administrator
14 shall make funds provided under this section available for
15 use by a recipient of a grant for a period of not less than
16 36 months.

17 “(g) AUTHORIZATION OF APPROPRIATIONS.—There
18 is authorized to be appropriated for grants under this sec-
19 tion \$800,000,000 for each of fiscal years 2021 through
20 2022.”.

21 **SEC. 602. STATE HOMELAND SECURITY GRANT PROGRAM.**

22 Section 2004 of the Homeland Security Act of 2002
23 (6 U.S.C. 605) is amended by striking subsection (f) and
24 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.

1 “(g) PERIOD OF PERFORMANCE.—The Adminis-
2 trator shall make funds provided under this section avail-
3 able for use by a recipient of a grant for a period of not
4 less than 36 months.

5 “(h) AUTHORIZATION OF APPROPRIATIONS.—There
6 is authorized to be appropriated for grants under this sec-
7 tion \$600,000,000 for each of fiscal years 2021 through
8 2022.”.

9 **SEC. 603. GRANTS TO DIRECTLY ELIGIBLE TRIBES.**

10 Section 2005 of the Homeland Security Act of 2002
11 (6 U.S.C. 606) is amended by—

12 (1) redesignating subsections (h) through (k) as
13 subsections (i) through (l), respectively; and

14 (2) inserting after subsection (g) the following
15 new subsection:

16 “(h) PERIOD OF PERFORMANCE.—The Secretary
17 shall make funds provided under this section available for
18 use by a recipient of a grant for a period of not less than
19 36 months.”.

20 **SEC. 604. LAW ENFORCEMENT TERRORISM PREVENTION.**

21 (a) LAW ENFORCEMENT TERRORISM PREVENTION
22 PROGRAM.—Subsection (a) of section 2006 of the Home-
23 land Security Act of 2002 (6 U.S.C. 607) is amended—

24 (1) in paragraph (1)—

1 (A) by inserting “States and high-risk
2 urban areas expend” after “that”; and

3 (B) by striking “is used”;

4 (2) in paragraph (2), by amending subpara-
5 graph (I) to read as follows:

6 “(I) activities as determined appropriate
7 by the Administrator, in coordination with the
8 Assistant Secretary for State and Local Law
9 Enforcement within the Office of Partnership
10 and Engagement of the Department, through
11 outreach to relevant stakeholder organizations;
12 and”; and

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

15 “(4) ANNUAL REPORT.—The Administrator, in
16 coordination with the Assistant Secretary for State
17 and Local Law Enforcement, shall report annually
18 from fiscal year 2021 through fiscal year 2022 on
19 the use of grants under sections 2003 and 2004 for
20 law enforcement terrorism prevention activities au-
21 thorized under this section, including the percentage
22 and dollar amount of funds used for such activities
23 and the types of projects funded.”.

1 (b) OFFICE FOR STATE AND LOCAL LAW ENFORCE-
2 MENT.—Subsection (b) section 2006 of the Homeland Se-
3 curity Act of 2002 (6 U.S.C. 607) is amended—

4 (1) in paragraph (1), by striking “Policy Direc-
5 torate” and inserting “Office of Partnership and
6 Engagement”

7 (2) in paragraph (4)—

8 (A) in subparagraph (B), by inserting “,
9 including through consultation with such agen-
10 cies regarding Department programs that may
11 impact such agencies” before the semicolon at
12 the end; and

13 (B) in subparagraph (D), by striking “en-
14 sure” and inserting “certify”.

15 **SEC. 605. PRIORITIZATION.**

16 (a) IN GENERAL.—Subsection (a) of section 2007 of
17 the Homeland Security Act of 2002 (6 U.S.C. 608) is
18 amended—

19 (1) in paragraph (1)—

20 (A) by amending subparagraph (A) to read
21 as follows:

22 “(A) its population, including consideration
23 of domestic and international tourists, com-
24 muters, and military populations, including

1 military populations residing in communities
2 outside military installations;”;

3 (B) in subparagraph (E), by inserting “,
4 including threat information from other rel-
5 evant Federal agencies and field offices, as ap-
6 propriate” before the semicolon at the end; and

7 (C) in subparagraph (I), by striking “tar-
8 get” and inserting “core”; and

9 (2) in paragraph (2), by striking “target” and
10 inserting “core”.

11 (b) REVIEW.—Not later than 90 days after the date
12 of the enactment of this Act, the Secretary of Homeland
13 Security, through the Administrator of the Federal Emer-
14 gency Management Agency, shall review and report to the
15 Committee on Homeland Security and the Committee on
16 Appropriations of the House of Representatives and the
17 Committee on Homeland Security and Governmental Af-
18 fairs and the Committee on Appropriations of the Senate
19 on the risk formula and methodology used to award grants
20 under sections 2003 and 2004 of the Homeland Security
21 Act of 2002 (6 U.S.C. 604 and 605), including a discus-
22 sion of any necessary changes to such formula to ensure
23 grant awards are appropriately based on risk.

24 (c) COMPTROLLER GENERAL REVIEW.—Not later
25 than 180 days after the date of enactment of this Act,

1 the Comptroller General of the United States shall review
2 and assess the risk formula and methodology used to
3 award grants under sections 2003 and 2004 of the Home-
4 land Security Act of 2002, including—

5 (1) the process utilized by the Department of
6 Homeland Security to gather threat information for
7 each potential State and high-risk urban area;

8 (2) the extent to which such risk formula and
9 methodology considers the factors specified in sec-
10 tion 2007 of the Homeland Security Act of 2002 (6
11 U.S.C. 608), in particular—

12 (A) the extent to which the jurisdiction has
13 unmet core capabilities due to resource con-
14 straints;

15 (B) the degree to which a jurisdiction has
16 been able to address capability gaps with pre-
17 vious grant awards; and

18 (C) in the case of a high-risk urban area,
19 the extent to which such high-risk urban area
20 includes—

21 (i) incorporated municipalities, coun-
22 ties, parishes, and Indian Tribes within the
23 relevant eligible metropolitan area the in-
24 clusion of which will enhance regional ef-
25 forts to prevent, prepare for, protect

- 1 against, and respond to acts of terrorism;
2 and
3 (ii) other local and Tribal govern-
4 ments in the surrounding area that are
5 likely to be called upon to respond to acts
6 of terrorism within the high-risk urban
7 area; and
8 (3) how grant award amounts are determined.

9 **SEC. 606. ALLOWABLE USES.**

10 Section 2008 of the Homeland Security Act of 2002
11 (6 U.S.C. 609) is amended—

12 (1) in subsection (a)—

13 (A) in the matter preceding paragraph (1),
14 by striking “target” and inserting “core”;

15 (B) by redesignating paragraphs (6)
16 through (14) as paragraphs (8) through (16),
17 respectively;

18 (C) in paragraph (5), by inserting before
19 the semicolon at the end the following: “, pro-
20 vided such purchases align with the Statewide
21 Communication Interoperability Plan and are
22 coordinated with the Statewide Interoperability
23 Coordinator or Statewide interoperability gov-
24 ernance body of the State of the recipient”; and

1 (D) by inserting after paragraph (5) the
2 following new paragraphs:

3 “(6) enhancing medical preparedness, medical
4 surge capacity, and mass prophylaxis capabilities, in-
5 cluding the development and maintenance of an ini-
6 tial pharmaceutical stockpile, including medical kits
7 and diagnostics sufficient to protect first responders,
8 their families, immediate victims, and vulnerable
9 populations from a chemical or biological event;

10 “(7) enhancing cybersecurity, including pre-
11 paring for and responding to cybersecurity risks and
12 incidents (as such terms are defined in section 227)
13 and developing statewide cyber threat information
14 analysis and dissemination activities;”;

15 (E) in paragraph (8), as so redesignated,
16 by striking “Homeland Security Advisory Sys-
17 tem” and inserting “National Terrorism Advi-
18 sory System”; and

19 (F) in paragraph (14), as so redesignated,
20 by striking “3” and inserting “5”;

21 (2) in subsection (b)—

22 (A) in paragraph (3)(B), by striking
23 “(a)(10)” and inserting “(a)(12)”; and

24 (B) in paragraph (4)(B)(i), by striking
25 “target” and inserting “core”; and

1 rity Appropriations Act, 2007; Public Law 109–295) and
2 Threat and Hazard Identification and Risk Assessments
3 required under subsections (e) and (f) of such sections
4 2003 and 2004, respectively, as added by this title, from
5 each State and high-risk urban area, the Administrator
6 of the Federal Emergency Management Agency shall con-
7 duct and submit to the Committee on Homeland Security
8 and the Committee on Transportation and Infrastructure
9 of the House of Representatives and the Committee on
10 Homeland Security and Governmental Affairs of the Sen-
11 ate an assessment of information provided in such Reports
12 and Assessments.

13 (b) ASSESSMENT REQUIREMENTS.—The assessment
14 required under subsection (a) shall include a comparison
15 of successive State Preparedness Reports and Threat and
16 Hazard Identification and Risk Assessments that aggre-
17 gates results across the States and high-risk urban areas.

18 **SEC. 609. GRANT MANAGEMENT BEST PRACTICES.**

19 The Administrator of the Federal Emergency Man-
20 agement Agency shall include in the annual Notice of
21 Funding Opportunity relating to grants under sections
22 2003 and 2004 of the Homeland Security Act of 2002
23 (6 U.S.C. 604 and 605) an appendix that includes the fol-
24 lowing:

1 (1) A summary of findings identified by the Of-
2 fice of the Inspector General of the Department of
3 Homeland Security in audits of such grants and
4 methods to address areas identified for improve-
5 ment, including opportunities for technical assist-
6 ance.

7 (2) Innovative projects and best practices insti-
8 tuted by grant recipients.

9 **SEC. 610. PROHIBITION ON CONSOLIDATION.**

10 The Secretary of Homeland Security may not imple-
11 ment the National Priorities Security Grant Program or
12 any successor consolidated grant program unless the Sec-
13 retary receives prior authorization from Congress permit-
14 ting such implementation.

15 **SEC. 611. MAINTENANCE OF GRANT INVESTMENTS.**

16 Section 2008 of the Homeland Security Act of 2002
17 (6 U.S.C. 609), as amended by this title, is further amend-
18 ed by adding at the end the following new subsection:

19 “(h) MAINTENANCE OF EQUIPMENT.—Any applicant
20 for a grant under section 2003 or 2004 seeking to use
21 funds to purchase equipment, including pursuant to para-
22 graphs (3), (4), (5), or (12) of subsection (a) of this sec-
23 tion, shall by the time of the receipt of such grant develop
24 a plan for the maintenance of such equipment over its life-

1 cycle that includes information identifying which entity is
2 responsible for such maintenance.”.

3 **SEC. 612. ALLOWABLE USES OF FUNDS FOR PUBLIC TRANS-**
4 **PORTATION SECURITY ASSISTANCE GRANTS.**

5 Subparagraph (A) of section 1406(b)(2) of the Imple-
6 menting Recommendations of the 9/11 Commission Act of
7 2007 (6 U.S.C. 1135(b)(2)(A); Public Law 110–53) is
8 amended by inserting “and associated backfill” after “se-
9 curity training”.

10 **SEC. 613. PERIODS OF PERFORMANCE FOR PUBLIC TRANS-**
11 **PORTATION SECURITY ASSISTANCE GRANTS.**

12 Section 1406 of the Implementing Recommendations
13 of the 9/11 Commission Act of 2007 (6 U.S.C. 1135; Pub-
14 lic Law 110–53) is amended by striking subsection (m)
15 and inserting the following new subsections:

16 “(m) PERIODS OF PERFORMANCE.—

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

23 “(2) EXCEPTION.—Funds provided pursuant to
24 a grant awarded under this section for a use speci-
25 fied in subparagraph (M) or (N) of subsection (b)(1)

1 shall remain available for use by a grant recipient
2 for a period of not fewer than 55 months.

3 “(n) AUTHORIZATION OF APPROPRIATIONS.—There
4 is authorized to be appropriated for grants under this sec-
5 tion \$200,000,000 for each of fiscal years 2021 through
6 2022.”.

7 **SEC. 614. COMPTROLLER GENERAL REVIEW OF PUBLIC**
8 **TRANSPORTATION SECURITY ASSISTANCE**
9 **GRANT PROGRAM.**

10 (a) IN GENERAL.—The Comptroller General of the
11 United States shall conduct a review of the public trans-
12 portation security assistance grant program under section
13 1406 of the Implementing Recommendations of the 9/11
14 Commission Act of 2007 (6 U.S.C. 1135; Public Law
15 110–53).

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

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

21 (2) An assessment of the manner in which such
22 projects address threats to public transportation in-
23 frastructure.

24 (3) An assessment of the impact, if any, of this
25 Act (including the amendments made by this Act) on

1 types of projects funded under the public transpor-
2 tation security assistance grant program.

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

6 (5) Recommendations to improve the manner in
7 which public transportation security assistance grant
8 program funds address vulnerabilities in public
9 transportation infrastructure.

10 (6) Recommendations to improve the manage-
11 ment and administration of the public transportation
12 security assistance grant program.

13 (c) REPORT.—Not later than 1 year after the date
14 of the enactment of this Act and again not later than five
15 years after such date of enactment, the Comptroller Gen-
16 eral shall submit to the Committee on Homeland Security
17 of the House of Representatives and the Committee on
18 Homeland Security and Governmental Affairs of the Sen-
19 ate a report on the review required under this section.

20 **SEC. 615. PORT SECURITY GRANT PROGRAM.**

21 Section 70107 of title 46, United States Code, is
22 amended by—

23 (1) striking subsection (l);

24 (2) redesignating subsection (m) as subsection

25 (l); and

1 (3) by adding at the end the following new sub-
2 sections:

3 “(n) PERIOD OF PERFORMANCE.—The Secretary
4 shall make funds provided under this section available for
5 use by a recipient of a grant for a period of not less than
6 36 months.

7 “(o) AUTHORIZATION OF APPROPRIATIONS.—There
8 is authorized to be appropriated for grants under this sec-
9 tion \$200,000,000 for each of fiscal years 2021 through
10 2022.”.

11 **SEC. 616. CYBER PREPAREDNESS.**

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

14 (1) in subsection (c)—

15 (A) in paragraph (5)(B), by inserting “,
16 including State, local, and regional fusion cen-
17 ters, as appropriate” before the semicolon at
18 the end;

19 (B) in paragraph (7), in the matter pre-
20 ceeding subparagraph (A), by striking “informa-
21 tion and recommendations” each place it ap-
22 pears and inserting “information, recommenda-
23 tions, and best practices”; and

24 (C) in paragraph (9), by inserting “best
25 practices,” after “defensive measures,”; and

1 (2) in subsection (d)(1)(B)(ii), by inserting
2 “and State, local, and regional fusion centers, as ap-
3 propriate” before the semicolon at the end.

4 (b) SENSE OF CONGRESS.—It is the sense of Con-
5 gress that to facilitate the timely dissemination to appro-
6 priate State, local, and private sector stakeholders of
7 homeland security information related to cyber threats,
8 the Secretary of Homeland Security should, to the great-
9 est extent practicable, work to share actionable informa-
10 tion in an unclassified form related to such threats.

11 **SEC. 617. OPERATION STONEGARDEN.**

12 (a) IN GENERAL.—Subtitle A of title XX of the
13 Homeland Security Act of 2002 (6 U.S.C. 601 et seq.)
14 is amended by adding at the end the following new section:

15 **“SEC. 2009. OPERATION STONEGARDEN.**

16 “(a) ESTABLISHMENT.—There is established in the
17 Department a program to be known as ‘Operation
18 Stonegarden’, under which the Secretary, acting through
19 the Administrator, shall make grants to eligible law en-
20 forcement agencies, through the State administrative
21 agency, to enhance border security in accordance with this
22 section.

23 “(a) ELIGIBLE RECIPIENTS.—To be eligible to re-
24 ceive a grant under this section, a law enforcement agen-
25 cy—

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.

1 “(c) PERIOD OF PERFORMANCE.—The Secretary
2 shall award grants under this section to grant recipients
3 for a period of not less than 36 months.

4 “(d) REPORT.—For each of fiscal years 2021 and
5 2022, the Administrator shall submit to the Committee
6 on Homeland Security and Governmental Affairs of the
7 Senate and the Committee on Homeland Security of the
8 House of Representatives a report that contains informa-
9 tion on the expenditure of grants made under this section
10 by each grant recipient.

11 “(e) AUTHORIZATION OF APPROPRIATIONS.—There
12 is authorized to be appropriated \$110,000,000 for each
13 of fiscal years 2021 and 2022 for grants under this sec-
14 tion.”.

15 (b) CONFORMING AMENDMENT.—Subsection (a) of
16 section 2002 of the Homeland Security Act of 2002 (6
17 U.S.C. 603) is amended to read as follows:

18 “(a) GRANTS AUTHORIZED.—The Secretary, through
19 the Administrator, may award grants under sections 2003,
20 2004, 2009, and 2010 to State, local, and Tribal govern-
21 ments, as appropriate.”.

22 (c) CLERICAL AMENDMENT.—The table of contents
23 in section 1(b) of the Homeland Security Act of 2002 is
24 amended by inserting after the item relating to section
25 2008 the following new item:

“Sec. 2009. Operation Stonegarden.”.

1 **Subtitle B—Communications**

2 **SEC. 621. OFFICE OF EMERGENCY COMMUNICATIONS.**

3 The Secretary of Homeland Security may not change
4 the location or reporting structure of the Office of Emer-
5 gency Communications of the Department of Homeland
6 Security unless the Secretary receives prior authorization
7 from the Committee on Homeland Security of the House
8 of Representatives and the Committee on Homeland Secu-
9 rity and Governmental Affairs of the Senate permitting
10 such change.

11 **SEC. 622. RESPONSIBILITIES OF OFFICE OF EMERGENCY** 12 **COMMUNICATIONS DIRECTOR.**

13 (a) IN GENERAL.—Subsection (c) of section 1801 of
14 the Homeland Security Act of 2002 (6 U.S.C. 571) is
15 amended—

16 (1) by striking paragraph (3);

17 (2) by redesignating paragraphs (4) through
18 (16) as paragraphs (3) through (15), respectively;

19 (3) in paragraph (8), as so redesignated, by
20 striking “, in cooperation with the National Commu-
21 nications System,”;

22 (4) in paragraph (11), as so redesignated, by
23 striking “Assistant Secretary for Grants and Train-
24 ing” and inserting “Administrator of the Federal
25 Emergency Management Agency”;

1 (5) in paragraph (14), as so redesignated, by
2 striking “and” at the end;

3 (6) in paragraph (15), as so redesignated, by
4 striking the period at the end and inserting a semi-
5 colon; and

6 (7) by adding at the end the following new
7 paragraphs:

8 “(16) administer the Government Emergency
9 Telecommunications Service (GETS) and Wireless
10 Priority Service (WPS) programs, or successor pro-
11 grams; and

12 “(17) assess the impact of emerging tech-
13 nologies on interoperable emergency communica-
14 tions.”.

15 (b) PERFORMANCE OF PREVIOUSLY TRANSFERRED
16 FUNCTIONS.—Subsection (d) of section 1801 of the
17 Homeland Security Act of 2002 is amended by—

18 (1) striking paragraph (2); and

19 (2) redesignating paragraph (3) as paragraph
20 (2).

21 **SEC. 623. ANNUAL REPORTING ON ACTIVITIES OF THE OF-**
22 **FICE OF EMERGENCY COMMUNICATIONS.**

23 Subsection (f) of section 1801 of the Homeland Secu-
24 rity Act of 2002 (6 U.S.C. 571) is amended to read as
25 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

1 (B) by inserting after paragraph (2) the
2 following new paragraph:

3 “(3) consider the impact of emerging tech-
4 nologies on the attainment of interoperable emer-
5 gency communications;”.

6 **SEC. 625. TECHNICAL EDIT.**

7 Paragraph (1) of section 1804(b) of the Homeland
8 Security Act of 2002 (6 U.S.C. 574(b)), in the matter pre-
9 ceding subparagraph (A), by striking “Assistant Secretary
10 for Grants and Planning” and inserting “Administrator
11 of the Federal Emergency Management Agency”.

12 **SEC. 626. PUBLIC SAFETY BROADBAND NETWORK.**

13 The Director of the Cybersecurity and Infrastructure
14 Security Agency of the Department of Homeland Security
15 shall provide to the Committee on Homeland Security and
16 the Committee on Energy and Commerce of the House
17 of Representatives and the Committee on Homeland Secu-
18 rity and Governmental Affairs of the Senate information
19 on the Department of Homeland Security’s responsibilities
20 related to the development of the nationwide Public Safety
21 Broadband Network authorized in section 6202 of the
22 Middle Class Tax Relief and Job Creation Act of 2012
23 (47 U.S.C. 1422; Public Law 112–96), including informa-
24 tion on efforts by the Department to work with the First
25 Responder Network Authority of the Department of Com-

1 merce to identify and address cyber risks that could im-
2 pact the near term or long term availability and operations
3 of such network and recommendations to mitigate such
4 risks.

5 **SEC. 627. COMMUNICATIONS TRAINING.**

6 The Under Secretary for Management of the Depart-
7 ment of Homeland Security, in coordination with the ap-
8 propriate component heads, shall develop a mechanism,
9 consistent with the strategy required pursuant to section
10 4 of the Department of Homeland Security Interoperable
11 Communications Act (Public Law 114–29; 6 U.S.C. 194
12 note), to verify that radio users within the Department
13 receive initial and ongoing training on the use of the radio
14 systems of such components, including interagency radio
15 use protocols.

16 **Subtitle C—Federal Emergency**
17 **Management Agency (FEMA)**

18 **SEC. 631. SHORT TITLE.**

19 This subtitle may be cited as the “FEMA Reauthor-
20 ization Act of 2019”.

21 **SEC. 632. REAUTHORIZATION OF FEDERAL EMERGENCY**
22 **MANAGEMENT AGENCY.**

23 Section 699 of the Post-Katrina Emergency Manage-
24 ment Reform Act of 2006 (Public Law 109–295; 6 U.S.C.
25 811) is amended—

1 (1) by striking “administration and operations”
2 each place it appears and inserting “management
3 and administration”;

4 (2) in paragraph (2), by striking “; and”;

5 (3) in paragraph (3), by striking the period and
6 inserting “; and”; and

7 (4) by adding at the end the following:

8 “(4) for fiscal year 2021, \$1,124,242,980; and

9 “(6) for fiscal year 2022, \$1,146,727,840.”.

10 **SEC. 633. NATIONAL DOMESTIC PREPAREDNESS CONSOR-**
11 **TIUM.**

12 Section 1204 of the Implementing Recommendations
13 of the 9/11 Commission Act (6 U.S.C. 1102) is amend-
14 ed—

15 (1) in subsection (b)(4), by striking “Rescue”
16 and inserting “Recovery”;

17 (2) in subsection (c), by inserting “to the extent
18 practicable, provide training in settings that simu-
19 late real response environments, such as urban
20 areas,” after “levels,”;

21 (3) in subsection (d), by striking paragraphs
22 (1) and (2) and inserting the following:

23 “(1) for the Center for Domestic Prepared-
24 ness—

25 “(A) \$68,131,920 for fiscal year 2021; and

1 “(B) \$69,494,558 for fiscal year 2022; and

2 “(2) for the members referred to in paragraphs

3 (2) through (7) of subsection (b)—

4 “(A) \$103,020,000 for fiscal year 2021;

5 and

6 “(B) \$105,080,400 for fiscal year 2022.”;

7 and

8 (4) in subsection (e) by striking—

9 (A) “each of the following entities” and in-
10 sserting “members enumerated in section (b)”;

11 (B) “2007—” and inserting “2015.”; and

12 (C) paragraphs (1) through (5).

13 **SEC. 634. RURAL DOMESTIC PREPAREDNESS CONSORTIUM.**

14 (a) **IN GENERAL.**—The Secretary of Homeland Secu-
15 rity is authorized to establish a Rural Domestic Prepared-
16 ness Consortium within the Department of Homeland Se-
17 curity consisting of universities and nonprofit organiza-
18 tions qualified to provide training to emergency response
19 providers from rural communities.

20 (b) **DUTIES.**—The Rural Domestic Preparedness
21 Consortium authorized under subsection (a) shall identify,
22 develop, test, and deliver training to State, local, and Trib-
23 al emergency response providers from rural communities,
24 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-

1 cessfully partner with other Blue Campaign compo-
2 nents; and

3 “(6) perform any other duties as assigned by
4 the Administrator.”.

5 (b) CLERICAL AMENDMENT.—The table of contents
6 in section 1(b) of the Homeland Security Act of 2002 is
7 amended by inserting after the item relating to section
8 528 the following new item:

 “Sec. 529. Center for Faith-Based and Neighborhood Partnerships.”.

9 **SEC. 636. EMERGENCY SUPPORT FUNCTIONS.**

10 (a) UPDATE.—Paragraph (13) of section 504(a) of
11 the Homeland Security Act of 2002 (6 U.S.C. 314(a)) is
12 amended by inserting “, periodically updating (but not less
13 often than once every five years),” after “administering”.

14 (b) EMERGENCY SUPPORT FUNCTIONS.—Section
15 653 of the Post-Katrina Emergency Management Reform
16 Act of 2006 (6 U.S.C. 753; title VI of the Department
17 of Homeland Security Appropriations Act, 2007; Public
18 Law 109–295) is amended—

19 (1) by redesignating subsections (d) and (e) as
20 subsections (e) and (f), respectively; and

21 (2) by inserting after subsection (e) the fol-
22 lowing new subsection:

23 “(d) COORDINATION.—The President, acting through
24 the Administrator, shall develop and provide to Federal
25 departments and agencies with coordinating, primary, or

1 supporting responsibilities under the National Response
2 Framework performance metrics to ensure readiness to
3 execute responsibilities under the emergency support func-
4 tions of such Framework.”.

5 **SEC. 637. REVIEW OF NATIONAL INCIDENT MANAGEMENT**
6 **SYSTEM.**

7 Paragraph (2) of section 509(b) of the Homeland Se-
8 curity Act of 2002 (6 U.S.C. 319(b)) is amended, in the
9 matter preceding subparagraph (A), by inserting “, but
10 not less often than once every five years,” after “periodi-
11 cally”.

12 **SEC. 638. REMEDIAL ACTION MANAGEMENT PROGRAM.**

13 Section 650 of the Post-Katrina Emergency Manage-
14 ment Reform Act of 2006 (6 U.S.C. 750; title VI of the
15 Department of Homeland Security Appropriations Act,
16 2007; Public Law 109–295) is amended to read as follows:

17 **“SEC. 650. REMEDIAL ACTION MANAGEMENT PROGRAM.**

18 “(a) IN GENERAL.—The Administrator, in coordina-
19 tion with the National Council on Disability and the Na-
20 tional Advisory Council, shall establish a remedial action
21 management program to—

22 “(1) analyze training, exercises, and real world
23 events to identify lessons learned, corrective actions,
24 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.”.

1 **SEC. 639. STRATEGIC HUMAN CAPITAL PLAN.**

2 Subsection (c) of section 10102 of title 5, United
3 States Code, is amended by striking “2007” and inserting
4 “2021”.

5 **SEC. 640. OFFICE OF DISABILITY INTEGRATION AND CO-**
6 **ORDINATION.**

7 (a) OFFICE OF DISABILITY INTEGRATION AND CO-
8 ORDINATION.—

9 (1) IN GENERAL.—Section 513 of the Home-
10 land Security Act of 2002 (6 U.S.C. 321b) is
11 amended to read as follows:

12 **“SEC. 513. OFFICE OF DISABILITY INTEGRATION AND CO-**
13 **ORDINATION.**

14 “(a) IN GENERAL.—There is established within the
15 Federal Emergency Management Agency an Office of Dis-
16 ability Integration and Coordination, which shall be head-
17 ed by a Director.

18 “(b) MISSION.—The mission of the Office is to en-
19 sure that individuals with disabilities and other access and
20 functional needs are included in emergency management
21 activities throughout the Agency by providing guidance,
22 tools, methods, and strategies for the purpose of equal
23 physical program and effective communication access.

24 “(c) RESPONSIBILITIES.—In support of the mission
25 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 disabili-
10 ties;

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 disabili-
17 ties, 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-

1 formation accessible to individuals with hearing and
2 vision disabilities;

3 “(10) ensure the availability of accessible trans-
4 portation options for individuals with disabilities in
5 the event of an evacuation;

6 “(11) provide guidance and implement policies
7 to ensure that the rights and feedback of individuals
8 with disabilities regarding post-evacuation residency
9 and relocation are respected;

10 “(12) ensure that meeting the needs of individ-
11 uals with disabilities are included in the components
12 of the national preparedness system established
13 under section 644 of the Post-Katrina Emergency
14 Management Reform Act of 2006 (Public Law 109–
15 295; 120 Stat. 1425; 6 U.S.C. 744); and

16 “(13) perform any other duties as assigned by
17 the Administrator.

18 “(d) DIRECTOR.—After consultation with organiza-
19 tions representing individuals with disabilities, the Admin-
20 istrator shall appoint a Director. The Director shall report
21 directly to the Administrator, in order to ensure that the
22 needs of individuals with disabilities are being properly ad-
23 dressed in emergency preparedness and disaster relief.

24 “(e) ORGANIZATIONS REPRESENTING INDIVIDUALS
25 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.

1 **SEC. 641. FEMA SENIOR LAW ENFORCEMENT ADVISOR.**

2 (a) IN GENERAL.—Title V of the Homeland Security
3 Act of 2002 (6 U.S.C. 311 et seq.), as amended by this
4 title, is further amended by adding at the end the fol-
5 lowing new section:

6 **“SEC. 530. SENIOR LAW ENFORCEMENT ADVISOR.**

7 “(a) ESTABLISHMENT.—There is established in the
8 Agency a Senior Law Enforcement Advisor to serve as a
9 qualified expert to the Administrator for the purpose of
10 strengthening the Agency’s coordination among State,
11 local, and Tribal law enforcement.

12 “(b) QUALIFICATIONS.—The Senior Law Enforce-
13 ment Advisor shall have an appropriate background with
14 experience in law enforcement, intelligence, information
15 sharing, and other emergency response functions.

16 “(c) RESPONSIBILITIES.—The Senior Law Enforce-
17 ment Advisor shall—

18 “(1) coordinate on behalf of the Administrator
19 with the Office for State and Local Law Enforce-
20 ment under section 2006 for the purpose of ensuring
21 State, local, and Tribal law enforcement receive con-
22 sistent and appropriate consideration in policies,
23 guidance, training, and exercises related to pre-
24 venting, preparing for, protecting against, and re-
25 sponding to natural disasters, acts of terrorism, and
26 other man-made disasters within the United States;

1 “(2) work with the Administrator and the Of-
2 fice for State and Local Law Enforcement under
3 section 2006 to ensure grants to State, local, and
4 Tribal government agencies, including programs
5 under sections 2003, 2004, and 2006(a), appro-
6 priately focus on terrorism prevention activities; and

7 “(3) serve other appropriate functions as deter-
8 mined by the Administrator.”.

9 (b) CLERICAL AMENDMENT.—The table of contents
10 in section 1(b) of the Homeland Security Act of 2002 is
11 amended by inserting after the item relating to section
12 529, as added by this title, the following new item:

 “Sec. 530. Senior Law Enforcement Advisor.”.

13 **SEC. 642. TECHNICAL AMENDMENTS TO NATIONAL EMER-**
14 **GENCY MANAGEMENT.**

15 (a) HOMELAND SECURITY ACT OF 2002.—Title V of
16 the Homeland Security Act of 2002 (6 U.S.C. 501 et seq.)
17 is amended—

18 (1) in section 501(8) (6 U.S.C. 311(8))—

19 (A) by striking “National Response Plan”
20 each place it appears and inserting “National
21 Response Framework”; and

22 (B) by striking “502(a)(6)” and inserting
23 “504(a)(6)”;

1 (2) in section 503(b)(2)(A) (6 U.S.C. 313) by
2 inserting “and incidents impacting critical infra-
3 structure” before the semicolon;

4 (3) in section 504(a) (6 U.S.C. 314(a))—

5 (A) in paragraph (3) by striking “, includ-
6 ing—” and inserting “(that includes incidents
7 impacting critical infrastructure), including—”;

8 (B) in paragraph (4) by inserting “, in-
9 cluding incidents impacting critical infrastruc-
10 ture” before the semicolon;

11 (C) in paragraph (5) by striking “and
12 local” and inserting “local, and Tribal”;

13 (D) in paragraph (6) by striking “national
14 response plan” and inserting “national response
15 framework, which shall be reviewed and up-
16 dated as required but not less than every 5
17 years”;

18 (E) by redesignating paragraphs (7)
19 through (21) as paragraphs (8) through (22),
20 respectively;

21 (F) by inserting after paragraph (6) the
22 following:

23 “(7) developing integrated frameworks, to in-
24 clude consolidating existing Government plans ad-
25 dressing 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”;

1 (6) in section 509 (6 U.S.C. 319)—

2 (A) in subsection (b)—

3 (i) in paragraph (1)—

4 (I) by striking “National Re-
5 sponse Plan” and inserting “National
6 Response Framework, National Pro-
7 tection Framework, National Preven-
8 tion Framework, National Mitigation
9 Framework, National Recovery
10 Framework”;

11 (II) by striking “successor” and
12 inserting “successors”; and

13 (III) by striking “plan” at the
14 end of that paragraph and inserting
15 “framework”; and

16 (ii) in paragraph (2), by striking “Na-
17 tional Response Plan” each place it ap-
18 pears and inserting “National Response
19 Framework”; and

20 (B) in subsection (c)(1)—

21 (i) in subparagraph (A)—

22 (I) by striking “NATIONAL RE-
23 SPONSE PLAN” in the header and in-
24 serting “NATIONAL RESPONSE
25 FRAMEWORK”; and

1 (II) by striking “National Re-
2 sponse Plan” in the text and inserting
3 “National Response Framework”; and
4 (ii) in subparagraph (B), by striking
5 “National Response Plan” and inserting
6 “National Response Framework”;
7 (7) in section 510 (6 U.S.C. 320)—
8 (A) in subsection (a), by striking “enter
9 into a memorandum of understanding” and in-
10 sserting “partner”;
11 (B) in subsection (b)(1)(A), by striking
12 “National Response Plan” and inserting “Na-
13 tional Response Framework”; and
14 (C) in subsection (c), by striking “National
15 Response Plan” and inserting “National Re-
16 sponse Framework”;
17 (8) in section 515(c)(1) (6 U.S.C. 321d(c)(1)),
18 by striking “and local” each place it appears and in-
19 sserting “, local, and Tribal”;
20 (9) by striking section 524 (6 U.S.C. 321m);
21 and
22 (10) in section 525(a) (6 U.S.C. 321n), by
23 striking “Secretary” and inserting “Administrator”.
24 (b) POST-KATRINA EMERGENCY MANAGEMENT RE-
25 FORM ACT OF 2006.—

1 (1) CITATION CORRECTION.—Section 602(13)
2 of the Post-Katrina Emergency Management Reform
3 Act of 2006 (6 U.S.C. 701(13)) is amended by strik-
4 ing “502(a)(6)” and inserting “504(a)(6)”.

5 (2) CHANGE OF REFERENCE.—Chapter 1 of
6 subtitle C of title VI of the Post-Katrina Emergency
7 Management Reform Act of 2006 (Public Law 109–
8 295) is amended by striking “National Response
9 Plan” each place it appears and inserting “National
10 Response Framework”.

11 (c) SAVINGS CLAUSE.—The amendments made by
12 subsection (a) to section 503(b)(2)(A) and paragraphs (3)
13 and (4) of section 504(a) of the Homeland Security Act
14 of 2002 may not be construed as affecting the authority,
15 existing on the day before the date of enactment of this
16 division, of any other component of the Department of
17 Homeland Security or any other Federal department or
18 agency.

19 **Subtitle D—Genome Editing Threat** 20 **Assessment**

21 **SEC. 651. GENOME EDITING THREAT ASSESSMENT.**

22 (a) IN GENERAL.—Not later than 180 days after the
23 date of the enactment of this Act, the Assistant Secretary
24 for the Countering Weapons of Mass Destruction Office
25 of the Department of Homeland Security, in coordination

1 with the Under Secretary for Intelligence and Analysis of
2 the Department, the Under Secretary for the Science and
3 Technology Directorate of the Department, and other
4 Federal partners, as appropriate, shall develop a threat
5 assessment on the potential homeland security
6 vulnerabilities associated with genome modification and
7 editing. Such threat assessment shall include information
8 relating to the following:

9 (1) The dual-use of emerging biotechnology.

10 (2) The ability of gene editing to maliciously
11 proliferate infectious diseases and pandemics on
12 human, animal, and plant populations.

13 (3) The cybersecurity vulnerabilities in com-
14 puter systems analyzing genomic data.

15 (4) Privacy concerns associated with analyzing
16 genomic data.

17 (b) RECOMMENDATIONS.—Upon completion of the
18 threat assessment required under subsection (a), the Sec-
19 retary of Homeland Security shall make a determination
20 if any changes to future operations of the Department of
21 Homeland Security are required to address security
22 vulnerabilities identified in such assessment.

23 (c) REPORT.—Not later than 60 days after the com-
24 pletion of the threat assessment required under subsection
25 (a), the Secretary of Homeland Security shall, consistent

1 with the protection of classified information, 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 the findings
5 of such threat assessment, any identified recommenda-
6 tions, plans for incorporating such recommendations into
7 future operations of the Department of Homeland Secu-
8 rity, and any proposed legislative changes informed by
9 such threat assessment.

10 **TITLE VII—PANDEMIC**
11 **PREPAREDNESS**

12 **SEC. 701. CHIEF MEDICAL OFFICER.**

13 Section 1931 of the Homeland Security Act of 2002
14 (6 U.S.C. 587) is amended—

15 (1) in subsection (c)—

16 (A) in the matter preceding paragraph (1),
17 by inserting “and shall establish medical and
18 human, animal, and occupational health expo-
19 sure policy, guidance, strategies, and initia-
20 tives,” before “including—”;

21 (B) in paragraph (1), by inserting before
22 the semicolon at the end the following: “, in-
23 cluding advice on how to prepare for, protect
24 against, respond to, recover from, and mitigate
25 against the medical effects of terrorist attacks

1 or other high consequence events utilizing
2 chemical, biological, radiological, or nuclear
3 agents or explosives”;

4 (C) in paragraph (2), by inserting before
5 the semicolon at the end the following: “, in-
6 cluding coordinating the Department’s policy,
7 strategy, and preparedness for pandemics and
8 emerging infectious diseases”;

9 (D) in paragraph (4)—

10 (i) by inserting “emergency medical
11 services and medical first responder stake-
12 holders,” after “the medical community,”;
13 and

14 (ii) by striking “and” at the end;

15 (E) by redesignating paragraph (5) as
16 paragraph (9); and

17 (F) by inserting after paragraph (4) the
18 following new paragraphs:

19 “(5) ensuring that the workforce of the Depart-
20 ment has evidence-based policy, standards, require-
21 ments, and metrics for operational medicine pro-
22 grams;

23 “(6) directing and maintaining a coordinated
24 system for medical support for the Department’s
25 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”;

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

3 “(d) **MEDICAL LIAISONS.**—The Chief Medical Officer
4 may provide medical liaisons to the components of the De-
5 partment to provide subject matter expertise on medical
6 and public health issues and a direct link to the Chief
7 Medical Officer. Such expertise may include the following:

8 “(1) Providing guidance on health and medical
9 aspects of policy, planning, and operations.

10 “(2) Supporting the development and alignment
11 of medical and health systems.

12 “(3) Identifying—

13 “(A) common gaps in medical and health
14 standards, policy, or guidance; and

15 “(B) enterprise solutions to bridge such
16 gaps.”.

17 **SEC. 702. MEDICAL COUNTERMEASURES PROGRAM.**

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

21 **“SEC. 1932. MEDICAL COUNTERMEASURES.**

22 “(a) **IN GENERAL.**—The Secretary shall establish a
23 medical countermeasures program to facilitate personnel
24 readiness, and protection for the Department’s employees
25 and working animals and individuals in the Department’s

1 care and custody, in the event of a chemical, biological,
2 radiological, nuclear, or explosives attack, naturally occur-
3 ring disease outbreak, or pandemic, and to support De-
4 partment mission continuity.

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

9 “(1) develop Department-wide standards for
10 medical countermeasure storage, security, dis-
11 pensing, and documentation;

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

15 “(3) preposition appropriate medical counter-
16 measures in strategic locations nationwide, based on
17 threat and employee density, in accordance with ap-
18 plicable Federal statutes and regulations;

19 “(4) provide oversight and guidance on dis-
20 pensing of stockpiled medical countermeasures;

21 “(5) ensure rapid deployment and dispensing of
22 medical countermeasures in a chemical, biological,
23 radiological, nuclear, or explosives attack, naturally
24 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-

1 pile under subsection (d), the Chief Medical Officer shall
2 utilize, if available—

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

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

7 “(f) REPORT.—Not later than 180 days after the
8 date of the enactment of this section, the Chief Medical
9 Officer shall report to the Committee on Homeland Secu-
10 rity of the House of Representatives and the Committee
11 on Homeland Security and Governmental Affairs of the
12 Senate on progress in achieving the requirements of this
13 section.”.

14 (b) CLERICAL AMENDMENT.—The table of contents
15 in section 1(b) of the Homeland Security Act of 2002 is
16 amended by adding after the item relating to section 1931
17 the following new item:

“Sec. 1932. Medical countermeasures.”.

18 **SEC. 703. PERSONAL PROTECTIVE EQUIPMENT.**

19 (a) DEFINITIONS.—In this section:

20 (1) APPROPRIATE CONGRESSIONAL COMMIT-
21 TEES.—The term “appropriate congressional com-
22 mittees” means the Committee on Homeland Secu-
23 rity of the House of Representatives and the Com-
24 mittee on Homeland Security and Governmental Af-
25 fairs of the Senate.

1 (2) DEPARTMENT.—The term “Department”
2 means the Department of Homeland Security.

3 (3) PERSONAL PROTECTIVE EQUIPMENT.—The
4 term “personal protective equipment” includes pro-
5 tective gloves, masks, and any additional protective
6 equipment determined appropriate by the Secretary.

7 (4) SECRETARY.—The term “Secretary” means
8 the Secretary of Homeland Security.

9 (b) AVAILABILITY OF PERSONAL PROTECTIVE
10 EQUIPMENT FOR CERTAIN DEPARTMENT PERSONNEL.—

11 (1) IN GENERAL.—Not later than 90 days after
12 the date of the enactment of this Act, the Secretary
13 shall ensure the availability of an adequate supply of
14 personal protective equipment to equip personnel of
15 the Department and each component conducting op-
16 erations requiring contact with the public for use
17 during the COVID–19 global pandemic. Such per-
18 sonnel include the following:

19 (A) Transportation Security Officers.

20 (B) Explosives Detection Canine Handlers.

21 (C) Federal Air Marshals.

22 (D) Transportation Security Inspectors.

23 (E) Administration personnel involved in
24 operations of Visual Intermodal Prevention and
25 Response teams.

1 (F) U.S. Border Patrol agents.

2 (G) U.S. Customs and Border Protection
3 officers.

4 (H) Air and Marine Officers.

5 (I) U.S. Border Patrol Processing Coordi-
6 nators.

7 (J) Officers of the Federal Protective Serv-
8 ice.

9 (K) Secret Service Agents and officers.

10 (L) U.S. Immigration and Customs En-
11 forcement officers.

12 (M) Any other personnel determined ap-
13 propriate by the Secretary.

14 (2) JOB HAZARD ANALYSIS.—Not later than 30
15 days after the date of the enactment of this Act,
16 each Department component head shall—

17 (A) ensure the job hazard analysis of each
18 such component identifies the regular duties
19 and tasks required of relevant personnel to de-
20 termine the amount of personal protective
21 equipment required per shift to conduct speci-
22 fied duties and tasks; and

23 (B) provide to the Secretary such analysis.

24 (3) STORAGE.—Not later than 30 days after
25 the date of the enactment of this Act, each Depart-

1 ment component head shall identify and implement
2 appropriate best practices for storing personal pro-
3 tective equipment.

4 (4) MEASURES TO PROTECT CERTAIN FRONT-
5 LINE PERSONNEL.—Not later than 60 days after the
6 date of the enactment of this Act, each Department
7 component head shall identify and implement meas-
8 ures to augment existing Department facilities and
9 vehicles to protect frontline Department personnel
10 regularly interacting with or transporting individuals
11 in the public. Such measures shall include the imple-
12 mentation of technologies such as plexiglass barriers,
13 biometric technology, computed tomography, detec-
14 tion-at-range, and credential authentication tech-
15 nology utilizing digital camera technology.

16 (5) POLICIES.—Not later than 60 days after
17 the date of the enactment of this Act, the Secretary
18 shall develop or update, as appropriate, policies for
19 the workforce of the Department related to the use
20 and potential reuse and availability of personal pro-
21 tective equipment.

22 (6) REPORT TO CONGRESS.—The Secretary
23 shall report to the appropriate congressional commit-
24 tees regarding the implementation of this subsection.

1 (c) COVID-19 AFTER-ACTION REVIEW.—Not later
2 than 180 days after the date of the enactment of this Act,
3 the Secretary shall submit to the appropriate congres-
4 sional committees an after-action review to examine the
5 Department’s response and mitigation efforts related to
6 the COVID–19 global pandemic. Such review shall include
7 information relating to the following:

8 (1) The overall preparedness of the Department
9 and each of the Department components to respond
10 to the COVID–19 global pandemic, including pre-
11 paredness to continue to fulfill its mission and pro-
12 tect Department personnel, the public, the transpor-
13 tation system, ports of entry, and the border.

14 (2) Communication challenges related to effec-
15 tively engaging with the public, Department per-
16 sonnel, and appropriate Federal, State, local, Tribal,
17 and industry stakeholders.

18 (3) The effectiveness of existing authorities al-
19 lowing the Department to utilize weather and safety
20 leave policies, hazard pay, or other personnel man-
21 agement policies to protect Department personnel.

22 (4) Impacts on security functions, operations,
23 and other homeland security missions.

1 (5) The availability of personal protective equip-
2 ment for Department personnel and individuals in
3 the custody of the Department.

4 (6) The extent to which technologies to promote
5 less contact between Department personnel and the
6 public, such as the technologies referred to in sub-
7 section (d), were implemented, and any challenges or
8 impediments to such implementation.

9 (7) Recommendations for action to improve the
10 preparedness of the Department for future crises
11 and pandemics.

12 **SEC. 704. TELEWORKING ASSESSMENT.**

13 Not later than one year after the date of the enact-
14 ment of this Act, the Comptroller General of the United
15 States shall conduct a review of the capabilities of the De-
16 partment of Homeland Security to support Department-
17 wide teleworking activity during the COVID-19 pandemic.
18 Such review shall include the following:

19 (1) A description of how many employees in
20 each component of the Department engaged in tele-
21 working prior to the COVID-19 pandemic and how
22 many engaged in teleworking beginning in March
23 2020.

1 (2) An evaluation of the capabilities of each of
2 the components to support remote teleworking ac-
3 tivities during the COVID-19 pandemic.

4 (3) An evaluation of the security protocols and
5 guidance developed by the Department and the level
6 of compliance by employees with such protocols.

7 (4) An assessment of the major issues encoun-
8 tered by each component during the transition to
9 teleworking due to the COVID-19 pandemic.

10 (5) An assessment of the availability of assist-
11 ance with teleworking capabilities during the
12 COVID-19 pandemic.

13 (6) An assessment of the capability of the De-
14 partment to support teleworking by employees en-
15 gaged in responsibilities that require the review of
16 classified materials.

17 (7) Recommendations for improving teleworking
18 capabilities for all employees, including for employ-
19 ees engaged in responsibilities that require the re-
20 view of classified materials.

21 **SEC. 705. TRANSPORTATION SECURITY PUBLIC HEALTH**

22 **THREAT PREPAREDNESS.**

23 (a) **DEFINITIONS.**—In this section:

1 (1) ADMINISTRATION; TSA.—The terms “Ad-
2 ministration” and “TSA” mean the Transportation
3 Security Administration.

4 (2) ADMINISTRATOR.—The term “Adminis-
5 trator” means the Administrator of the Transpor-
6 tation Security Administration.

7 (3) APPROPRIATE CONGRESSIONAL COMMIT-
8 TEES.—The term “appropriate congressional com-
9 mittees” means—

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

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

16 (4) DEPARTMENT.—The terms “Department”
17 means the Department of Homeland Security.

18 (b) AUTHORIZATION OF TSA PERSONNEL DE-
19 TAILS.—

20 (1) IN GENERAL.—Pursuant to section 114(m)
21 of title 49, United States Code, the Administrator is
22 authorized to provide Administration personnel to
23 other components of the Department and other Fed-
24 eral agencies to improve coordination with such com-
25 ponents and such agencies to prepare for, protect

1 against, and respond to public health threats to
2 transportation security.

3 (2) STRATEGY.—Not later than 180 days after
4 the date of the enactment of this Act, the Adminis-
5 trator shall brief the appropriate congressional com-
6 mittees regarding a strategy to improve coordination
7 with other components of the Department and other
8 Federal agencies to prepare for, protect against, and
9 respond to public health threats to transportation
10 security.

11 (c) TSA PREPAREDNESS.—

12 (1) RISK ANALYSIS.—To the extent possible
13 and in consultation with transportation security
14 stakeholders, the Administrator shall conduct an
15 analysis of transportation sector preparedness for
16 public health threats. Such analysis shall assess at
17 a minimum the following:

18 (A) The risks of public health threats to
19 transportation security, including to transpor-
20 tation hubs, transportation security stake-
21 holders, Administration personnel, and pas-
22 sengers.

23 (B) Information sharing challenges among
24 relevant components of the Department, other

1 Federal agencies, international partners, and
2 transportation security stakeholders.

3 (C) Impacts on changes to Administration
4 policies and procedures for screening passengers
5 and property.

6 (2) BRIEFING TO CONGRESS.—Not later than
7 180 days after the date of the enactment of this Act,
8 the Administrator shall brief the appropriate con-
9 gressional committees on the following:

10 (A) The risk analysis required under para-
11 graph (1).

12 (B) Technologies necessary to advance to-
13 ward a contactless checkpoint to better protect
14 from future public health threats Administra-
15 tion personnel, passengers, airport personnel,
16 and authorized personnel who pass through air-
17 port screening areas.

18 (C) Policies and procedures implemented
19 by the Administration and transportation secu-
20 rity stakeholders to protect from public health
21 threats Administration personnel, passengers,
22 airport personnel, and authorized personnel who
23 pass through airport screening areas, as well as
24 future plans for additional measures relating to
25 such protection.

1 (D) The status of existing or future
2 planned security directives or emergency
3 amendments to air carrier security require-
4 ments for flights from international points.

5 (E) How the Administration coordinates
6 and shares information with relevant domestic
7 and international partners during a public
8 health threat, and how such coordination may
9 be improved.

10 **SEC. 706. SECURING CRITICAL SUPPLIES.**

11 (a) STRATEGY TO PREVENT A SHORTAGE OF ITEMS
12 DETERMINED TO BE CRITICAL TO SURVIVAL DURING A
13 CRISIS AND SAFEGUARD THE SUPPLY CHAINS OF SUCH
14 ITEMS.—Not later than 180 days after the date of the
15 enactment of this Act, the Secretary, acting through the
16 Under Secretary and the Director, shall—

17 (1) identify items determined by the Secretary
18 to be critical to survival during a crisis resulting
19 from a terrorist attack, pandemic, or natural dis-
20 aster;

21 (2) assess the activities of the Department with
22 respect to the prevention of a shortage of items;

23 (3) assess vulnerabilities in the supply chain for
24 such items, which vulnerabilities may be exploited by
25 individuals, entities, or foreign terrorist organiza-

1 tions that may have an adversarial relationship with
2 the United States; and

3 (4) develop and submit to the appropriate con-
4 gressional committees a—

5 (A) report containing a strategy to prevent
6 such a shortage based upon the assessments re-
7 quired under paragraph (2); and

8 (B) classified annex to the report required
9 under subparagraph (A) relating to a strategy
10 to prevent the exploitation of vulnerabilities in
11 the supply chain for such items based upon the
12 assessment required under paragraph (3).

13 (b) MATTERS INCLUDED.—The strategies required
14 under subsection (a) shall include—

15 (1) an identification of items that the Secretary
16 determines to be critical to survival, including—

17 (A) food and water;

18 (B) prescription medication;

19 (C) medical supplies; and

20 (D) energy infrastructure and supplies;

21 (2) an examination of whether the source of
22 any such item is foreign-owned, controlled, or influ-
23 enced by a country that may have an adversarial re-
24 lationship with the United States; and

1 (3) recommendations with respect to steps the
2 Department could take to—

3 (A) ensure the availability of such items;
4 and

5 (B) safeguard from exploitation by individ-
6 uals, entities, or foreign terrorist organizations
7 the supply chain for such items.

8 (c) DEFINITIONS.—In this section:

9 (1) APPROPRIATE CONGRESSIONAL COMMIT-
10 TEES.—The term “appropriate congressional com-
11 mittees” means—

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

14 (B) the Committee on Homeland Security
15 and Governmental Affairs of the Senate.

16 (2) DEPARTMENT.—The term “Department”
17 means the Department of Homeland Security.

18 (3) DIRECTOR.—The term “Director” means
19 the Director of the Cybersecurity and Infrastructure
20 Security Agency of the Department of Homeland Se-
21 curity.

22 (4) SECRETARY.—The term “Secretary” means
23 the Secretary of Homeland Security.

24 (5) UNDER SECRETARY.—The term “Under
25 Secretary” means the Under Secretary of Intel-

- 1 ligence and Analysis of the Department of Home-
- 2 land Security.