H. R. 6381

To provide for certain homeland security improvements, and for other purposes.

IN THE HOUSE OF REPRESENTATIVES

NOVEMBER 18, 2016

Mr. McCaul introduced the following bill; which was referred to the Committee on Homeland Security, and in addition to the Committees on Foreign Affairs, the Judiciary, Transportation and Infrastructure, Energy and Commerce, Agriculture, Oversight and Government Reform, Ways and Means, Science, Space, and Technology, and Financial Services, for a period to be subsequently determined by the Speaker, in each case for consideration of such provisions as fall within the jurisdiction of the committee concerned.

A BILL

To provide for certain homeland security improvements, and for other purposes.

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

SECTION 1. SHORT TITLE; TABLE OF CONTENTS.

(a) Short Title.—This Act may be cited as the “DHS Reform and Improvement Act”.

(b) Table of Contents.—The table of contents for this Act is as follows:

1. Be it enacted by the Senate and House of Representatives of the United States of America in Congress assembled,
2. Section 1. Short Title; Table of Contents.
3. (a) Short Title.—This Act may be cited as the “DHS Reform and Improvement Act”.
4. (b) Table of Contents.—The table of contents for this Act is as follows:
Sec. 1. Short title; table of contents.

TITLE I—HOMELAND SECURITY DRONE ASSESSMENT AND ANALYSIS

Sec. 101. Drone assessment and analysis.

TITLE II—BORDER AND MARITIME COORDINATION IMPROVEMENT

Sec. 201. U.S. Customs and Border Protection coordination.
Sec. 203. Public-private partnerships.
Sec. 204. Establishment of the Office of Biometric Identity Management.
Sec. 205. Cost-benefit analysis of co-locating operational entities.
Sec. 206. Strategic personnel plan for U.S. Customs and Border Protection personnel deployed abroad.
Sec. 207. Threat assessment for United States-bound international mail.
Sec. 208. Evaluation of Coast Guard Deployable Specialized Forces.
Sec. 209. Customs-Trade Partnership Against Terrorism improvement.
Sec. 210. Strategic plan to enhance the security of the international supply chain.
Sec. 211. Container Security Initiative.
Sec. 212. Transportation Worker Identification Credential waiver and appeals process.
Sec. 213. Repeals.

TITLE III—SECURING OUR AGRICULTURE AND FOOD

Sec. 301. Coordination of food, agriculture, and veterinary defense against terrorism.

TITLE IV—STRONG VISA INTEGRITY SECURES AMERICA

Sec. 401. Visa security.
Sec. 402. Electronic passport screening and biometric matching.
Sec. 403. Reporting of visa overstays.
Sec. 404. Student and exchange visitor information system verification.

TITLE V—PROMOTING RESILIENCE AND EFFICIENCY IN PREPARING FOR ATTACKS AND RESPONDING TO EMERGENCIES

Subtitle A—Grants, Training, Exercises, and Coordination

Sec. 501. Memoranda of understanding.
Sec. 503. Operation Stonegarden.
Sec. 504. Grants metrics.
Sec. 505. Grant management best practices.
Sec. 506. Administration and coordination of grants.
Sec. 507. Funding prohibition.
Sec. 508. Law enforcement terrorism prevention.
Sec. 509. Allowable uses.
Sec. 510. Maintenance of grant investments.
Sec. 512. Rural Domestic Preparedness Consortium.
Sec. 513. Emergency support functions.
Sec. 514. Review of National Incident Management System.

•HR 6381 IH
Sec. 515. Approval of certain equipment.
Sec. 516. Remedial action management program.

Subtitle B—Communications

Sec. 521. Office of Emergency Communications.
Sec. 522. Responsibilities of Office of Emergency Communications Director.
Sec. 523. Annual reporting on activities of the Office of Emergency Communications.
Sec. 524. National Emergency Communications Plan.
Sec. 525. Technical edits.
Sec. 526. Public Safety Broadband Network.
Sec. 527. Statewide interoperability coordinators.
Sec. 528. Communications training.

Subtitle C—Medical Preparedness

Sec. 531. Pre-event anthrax vaccination program for emergency response providers.
Sec. 532. Chief Medical Officer.
Sec. 533. Medical Countermeasures Program.

Subtitle D—Management

Sec. 541. Mission support.
Sec. 542. Systems modernization.
Sec. 543. Strategic human capital plan.
Sec. 544. Activities related to children.

Subtitle E—Flood Insurance Claims Process Reforms

Sec. 551. Claims adjustment and engineering reports.
Sec. 552. Judicial review.

TITLE VI—CYBERSECURITY AND INFRASTRUCTURE PROTECTION AGENCY

Sec. 601. Cybersecurity and Infrastructure Protection Agency.
Sec. 602. Establishment of the Office of Biometric Identity Management.
Sec. 603. Rule of construction.
Sec. 604. Prohibition on additional funding.

TITLE VII—STRENGTHENING CYBERSECURITY INFORMATION SHARING AND COORDINATION IN OUR PORT

Sec. 701. Improving cybersecurity risk assessments, information sharing, and coordination.
Sec. 702. Cybersecurity enhancements to maritime security activities.
Sec. 703. Vulnerability assessments and security plans.

TITLE VIII—STRENGTHENING STATE AND LOCAL CYBER CRIME FIGHTING


TITLE IX—DEPARTMENT OF HOMELAND SECURITY CBRNE DEFENSE

•HR 6381 IH
Sec. 901. CBRNE Office.
Sec. 902. Chemical Division.
Sec. 903. Biological Division.
Sec. 904. Nuclear Division.
Sec. 905. Explosives Division.
Sec. 906. Savings provisions.
Sec. 907. Clerical amendments.

TITLE X—GAINS IN GLOBAL NUCLEAR DETECTION ARCHITECTURE

Sec. 1001. Duties of the Domestic Nuclear Detection Office.

TITLE XI—UNITED STATES IMMIGRATION AND CUSTOMS ENFORCEMENT AUTHORIZATION

Sec. 1101. Establishment of United States Immigration and Customs Enforcement.

TITLE XII—FEDERAL LAW ENFORCEMENT TRAINING CENTERS REFORM AND IMPROVEMENT

Sec. 1201. Federal Law Enforcement Training Centers.

TITLE XIII—PREVENT TRAFFICKING IN CULTURAL PROPERTY

Sec. 1301. Definition.
Sec. 1302. Statement of policy.
Sec. 1304. Role of the Smithsonian Institution.
Sec. 1305. Report.

TITLE XIV—DEPARTMENT OF HOMELAND SECURITY HEADQUARTERS REFORM AND IMPROVEMENT

Sec. 1401. Prohibition on additional authorization of appropriations.

Subtitle A—Department of Homeland Security Headquarters Reauthorization

Sec. 1411. Definitions.
Sec. 1412. Headquarters components.
Sec. 1413. Chief Privacy Officer.
Sec. 1414. Office of Policy.
Sec. 1415. Quadrennial homeland security review.
Sec. 1416. Future years homeland security program.
Sec. 1417. Management and execution.
Sec. 1418. Chief Financial Officer.
Sec. 1419. Chief Procurement Officer.
Sec. 1420. Chief Information Officer.
Sec. 1421. Chief Human Capital Officer.
Sec. 1422. Chief Security Officer.
Sec. 1423. Cost savings and efficiency reviews.
Sec. 1424. Field efficiencies plan.
Sec. 1425. Resources to respond to operational surges.
Sec. 1426. Department of Homeland Security rotation program.

Subtitle B—Department of Homeland Security Acquisition Accountability and Efficiency
Sec. 1431. Definitions.

PART 1—ACQUISITION AUTHORITIES

Sec. 1441. Acquisition authorities for Under Secretary for Management.
Sec. 1442. Acquisition authorities for Chief Financial Officer.
Sec. 1443. Acquisition authorities for Chief Information Officer.
Sec. 1444. Requirements to ensure greater accountability for acquisition programs.

PART 2—ACQUISITION PROGRAM MANAGEMENT DISCIPLINE

Sec. 1451. Acquisition Review Board.
Sec. 1452. Requirements to reduce duplication in acquisition programs.
Sec. 1453. Government Accountability Office review of Board and of requirements to reduce duplication in acquisition programs.
Sec. 1454. Excluded Party List System waivers.
Sec. 1455. Inspector General oversight of suspension and debarment.

PART 3—ACQUISITION PROGRAM MANAGEMENT ACCOUNTABILITY AND TRANSPARENCY

Sec. 1461. Congressional notification and other requirements for major acquisition program breach.
Sec. 1462. Multiyear acquisition strategy.
Sec. 1463. Acquisition reports.
Sec. 1464. Government Accountability Office review of multiyear acquisition strategy.
Sec. 1465. Office of Inspector General report.

TITLE XV—QUADRENNIAL HOMELAND SECURITY REVIEW
TECHNICAL CORRECTION

Sec. 1501. Technical corrections to quadrennial homeland security review.

TITLE XVI—TERRORIST AND FOREIGN FIGHTER TRAVEL EXERCISE

Sec. 1601. Exercise on terrorist and foreign fighter travel.
Sec. 1602. Emerging threats in the national exercise program.

TITLE XVII—AIRPORT PERIMETER AND ACCESS CONTROL SECURITY

Sec. 1701. Risk assessments of airport security.
Sec. 1702. Airport security strategy development.

TITLE XVIII—COMMUNITY COUNTERTERRORISM PREPAREDNESS

Sec. 1801. Major metropolitan area counterterrorism training and exercise grant program.

TITLE XIX—CYBER PREPAREDNESS

Sec. 1901. Information sharing.
Sec. 1902. Homeland security grants.
Sec. 1903. Sense of Congress.

TITLE XX—TRANSIT SECURITY GRANT PROGRAM FLEXIBILITY
Sec. 2001. Allowable uses of funds for public transportation security assistance grants.
Sec. 2003. GAO review.

TITLE XXI—SUPPORT FOR RAPID INNOVATION

Sec. 2101. Cybersecurity research and development projects.

TITLE XXII—LEVERAGING EMERGING TECHNOLOGIES

Sec. 2201. Innovation engagement.

TITLE XXIII—FIRST RESPONDER ACCESS TO INNOVATIVE TECHNOLOGIES

Sec. 2301. Approval of certain equipment.

TITLE XXIV—DEPARTMENT OF HOMELAND SECURITY STRATEGY FOR INTERNATIONAL PROGRAMS

Sec. 2401. Comprehensive strategy for international programs for vetting and screening persons seeking to enter the United States.

TITLE XXV—DHS STOP ASSET AND VEHICLE EXCESS

Sec. 2601. DHS vehicle fleets.
Sec. 2602. GAO report and Inspector General review.

TITLE XXVI—COUNTERTERRORISM SCREENING AND ASSISTANCE

Sec. 2601. Foreign partner engagement plan.
Sec. 2602. Sharing systems and equipment to obstruct travel by terrorists and foreign fighters.
Sec. 2603. Actions with respect to foreign countries that fail to meet minimum standards for serious and sustained efforts to combat terrorist and foreign fighter travel.
Sec. 2604. Definitions.
Sec. 2605. Prohibition on additional funding.

TITLE XXVII—SOUTHWEST BORDER SECURITY THREAT ASSESSMENT

Sec. 2701. Southwest border threat analysis.
Sec. 2702. Border Patrol Strategic Plan.
Sec. 2703. Definitions.

TITLE XXVIII—NATIONAL STRATEGY TO COMBAT TERRORIST TRAVEL

Sec. 2801. National strategy to combat terrorist travel.

TITLE XXIX—STATE AND HIGH-RISK URBAN AREA WORKING GROUP

Sec. 2901. Administration and coordination of certain DHS grants.

TITLE XXX—STATE AND LOCAL CYBER PROTECTION
Sec. 3001. State and local coordination on cybersecurity with the National Cybersecurity and Communications Integration Center.

TITLE XXXI—FUSION CENTER ENHANCEMENT


TITLE XXXII—TRANSPORTATION SECURITY ADMINISTRATION REFORM AND IMPROVEMENT

Sec. 3201. Definitions.

Subtitle A—Aviation Security

Sec. 3211. TSA PreCheck.
Sec. 3212. PreCheck and general passenger biometric identification.
Sec. 3213. Limitation; PreCheck operations maintained; alternate methods.
Sec. 3214. Secure Flight program.
Sec. 3215. Efficiency review by TSA.
Sec. 3216. Donation of screening equipment to protect the United States.
Sec. 3217. Review of sustained security directives.
Sec. 3218. Maintenance of security-related technology.
Sec. 3219. Vetting of aviation workers.
Sec. 3220. Aviation Security Advisory Committee consultation.
Sec. 3221. Private contractor canine evaluation and integration pilot program.
Sec. 3222. Covert testing at airports.
Sec. 3223. Training for Transportation Security Officers.

Subtitle B—Surface Transportation Security and Other Matters

Sec. 3231. Surface Transportation Inspectors.
Sec. 3232. Inspector General audit; TSA Office of Inspection workforce certification.
Sec. 3234. Security training for frontline transportation workers.
Sec. 3235. Feasibility assessment.

TITLE XXXIII—DHS SCIENCE AND TECHNOLOGY REFORM AND IMPROVEMENT

Sec. 3301. Science and technology in support of homeland security.

TITLE XXXIV—REVIEW OF UNIVERSITY-BASED CENTERS

Sec. 3401. Review of university-based centers.
TITLE I—HOMELAND SECURITY

DRONE ASSESSMENT AND ANALYSIS

SEC. 101. DRONE ASSESSMENT AND ANALYSIS.

(a) IN GENERAL.—The Secretary of Homeland Security shall, in consultation with the Secretary of Defense, the Secretary of Transportation, the Secretary of Energy, and the Chairman of the Nuclear Regulatory Commission research how commercially available small- and medium-sized unmanned aircraft, excluding aircraft over 1,300 pounds, could be used to perpetuate an attack and, based on such research, the Secretary of Homeland Security shall develop policies, guidance, and protocols for the Department of Homeland Security to prevent such an attack or mitigate the risks of such an attack. Not later than 180 days after the completion of the research required under this subsection, the Secretary of Homeland Security may provide, as appropriate, the Secretary of Defense, the Secretary of Transportation, the Secretary of Energy, and the Chairman of the Nuclear Regulatory Commission information, based on such research, regarding how to best prevent and mitigate the risk of such an attack.

(b) DISSEMINATION TO STATE AND LOCAL OFFICIALS.—The Secretary of Homeland Security shall disseminate information to State, local, and tribal law en-
forcement officials and State and major urban area fusion
centers, as appropriate, regarding how such officials may
bolster preparedness for and responses to attacks per-
petrated by commercially available small- and medium-
sized unmanned aircraft, excluding aircraft over 1,300
pounds.

(e) REPORT.—Not later than 1 year after the date
of the enactment of this Act, the Secretary of Homeland
Security shall submit to the Committee on Homeland Se-
curity and the Committee on Transportation and Infra-
structure of the House of Representatives and the Com-
mittee on Homeland Security and Governmental Affairs
and the Committee on Commerce, Science, and Transpor-
tation of the Senate an assessment of the security risk
associated with commercially available small- and medium-
sized unmanned aircraft, excluding aircraft over 1,300
pounds. Such assessment shall be informed by research
conducted in accordance with subsection (a), shall contain
recommendations, if applicable, to prevent and mitigate
the risk of an unmanned aircraft system attack, and may
be developed in coordination with the Centers of Excel-
ience of the Department of Homeland Security and other
academic institutions.

(d) PROHIBITION ON NEW FUNDING.—No funds are
authorized to be appropriated to carry out this title. This
title shall be carried out using amounts appropriated or otherwise made available for such purposes.

**TITLE II—BORDER AND MARITIME COORDINATION IMPROVEMENT**

**SEC. 201. U.S. CUSTOMS AND BORDER PROTECTION COORDINATION.**

(a) In General.—Subtitle B of title IV of the Homeland Security Act of 2002 (6 U.S.C. 211 et seq.) is amended by adding at the end the following new section:

“**SEC. 420. IMMIGRATION COOPERATION PROGRAM.**

“(a) In General.—There is established within U.S. Customs and Border Protection a program to be known as the Immigration Cooperation Program. Under the Program, U.S. Customs and Border Protection officers, pursuant to an arrangement with the government of a foreign country, may cooperate with authorities of that government, air carriers, and security employees at airports located in that country, to identify persons who may be inadmissible to the United States or otherwise pose a risk to border security.

“(b) Activities.—In carrying out the program, U.S. Customs and Border Protection officers posted in a foreign country under subsection (a) may—
“(1) be stationed at airports in that country, including for purposes of conducting risk assessments and enhancing border security;

“(2) assist authorities of that government, air carriers, and security employees with document examination and traveler security assessments;

“(3) provide relevant training to air carriers, their security staff, and such authorities;

“(4) exchange information with, and provide technical assistance, equipment, and training to, such authorities to facilitate risk assessments of travelers and appropriate enforcement activities related to such assessments;

“(5) make recommendations to air carriers to deny boarding to potentially inadmissible travelers bound for the United States; and

“(6) conduct other activities, as appropriate, to protect the international borders of the United States and facilitate the enforcement of United States laws, as directed by the Commissioner of U.S. Customs and Border Protection.

“SEC. 420A. AIR CARGO ADVANCE SCREENING.

“The Commissioner of U.S. Customs and Border Protection shall—
“(1) consistent with the requirements enacted
by the Trade Act of 2002 (Public Law 107–210)—

“(A) establish a program for the collection
by U.S. Customs and Border Protection of ad-
ance electronic information from air carriers
and other persons and governments within the
supply chain regarding cargo being transported
to the United States by air; and

“(B) under such program, require that
such information be transmitted by such per-
sons and governments at the earliest point
practicable prior to loading of such cargo onto
an aircraft destined to or transiting through the
United States; and

“(2) coordinate with the Administrator for the
Transportation Security Administration to identify
opportunities where the information furnished in
compliance with the program established under this
section can be used to meet the requirements of a
program administered by the Administrator of the
Transportation Security Administration.
SEC. 420B. U.S. CUSTOMS AND BORDER PROTECTION OFFICE OF AIR AND MARINE OPERATIONS

ASSET DEPLOYMENT.

“(a) In General.—Any deployment of new assets by U.S. Customs and Border Protection’s Office of Air and Marine Operations following the date of the enactment of this section, shall, to the greatest extent practicable, occur in accordance with a risk-based assessment that considers mission needs, validated requirements, performance results, threats, costs, and any other relevant factors identified by the Commissioner of U.S. Customs and Border Protection. Specific factors to be included in such assessment shall include, at a minimum, the following:

“(1) Mission requirements that prioritize the operational needs of field commanders to secure the United States border and ports.

“(2) Other Department assets available to help address any unmet border and port security mission requirements, in accordance with paragraph (1).

“(3) Risk analysis showing positioning of the asset at issue to respond to intelligence on emerging terrorist or other threats.

“(4) Cost-benefit analysis showing the relative ability to use the asset at issue in the most cost-eff-
effective way to reduce risk and achieve mission success.

“(b) CONSIDERATIONS.—An assessment required under subsection (a) shall consider applicable Federal guidance, standards, and agency strategic and performance plans, including the following:

“(1) The most recent departmental Quadrennial Homeland Security Review under section 707, and any follow-up guidance related to such Review.

“(2) The Department’s Annual Performance Plans.

“(3) Department policy guiding use of integrated risk management in resource allocation decisions.

“(4) Department and U.S. Customs and Border Protection Strategic Plans and Resource Deployment Plans.

“(5) Applicable aviation guidance from the Department, including the DHS Aviation Concept of Operations.

“(6) Other strategic and acquisition guidance promulgated by the Federal Government as the Secretary determines appropriate.

“(c) AUDIT AND REPORT.—The Inspector General of the Department shall biennially audit the deployment of
new assets by U.S. Customs and Border Protection's Office of Air and Marine Operations and submit to the Committee on Homeland Security of the House of Representatives and the Committee on Homeland Security and Governmental Affairs of the Senate a report on the compliance of the Department with the requirements of this section.

“(d) Marine Interdiction Stations.—Not later than 180 days after the date of the enactment of this section, the Commissioner of U.S. Customs and Border Protection shall submit to the Committee on Homeland Security of the House of Representatives and the Committee on Homeland Security and Governmental Affairs of the Senate an identification of facilities owned by the Federal Government in strategic locations along the maritime border of California that may be suitable for establishing additional Office of Air and Marine Operations marine interdiction stations.

“SEC. 420C. INTEGRATED BORDER ENFORCEMENT TEAMS.

“(a) Establishment.—The Secretary shall establish within the Department a program to be known as the Integrated Border Enforcement Team program (referred to in this section as ‘IBET’).
“(b) PURPOSE.—The Secretary shall administer the IBET program in a manner that results in a cooperative approach between the United States and Canada to—

“(1) strengthen security between designated ports of entry;

“(2) detect, prevent, investigate, and respond to terrorism and violations of law related to border security;

“(3) facilitate collaboration among components and offices within the Department and international partners;

“(4) execute coordinated activities in furtherance of border security and homeland security; and

“(5) enhance information-sharing, including the dissemination of homeland security information among such components and offices.

“(c) COMPOSITION AND LOCATION OF IBETS.—

“(1) COMPOSITION.—IBETs shall be led by the United States Border Patrol and may be comprised of personnel from the following:

“(A) Other subcomponents of U.S. Customs and Border Protection.

“(B) U.S. Immigration and Customs Enforcement, led by Homeland Security Investigations.
“(C) The Coast Guard, for the purpose of securing the maritime borders of the United States.

“(D) Other Department personnel, as appropriate.

“(E) Other Federal departments and agencies, as appropriate.

“(F) Appropriate State law enforcement agencies.

“(G) Foreign law enforcement partners.

“(H) Local law enforcement agencies from affected border cities and communities.

“(I) Appropriate tribal law enforcement agencies.

“(2) LOCATION.—The Secretary is authorized to establish IBETs in regions in which such teams can contribute to IBET missions, as appropriate. When establishing an IBET, the Secretary shall consider the following:

“(A) Whether the region in which the IBET would be established is significantly impacted by cross-border threats.

“(B) The availability of Federal, State, local, tribal, and foreign law enforcement resources to participate in an IBET.
“(C) Whether, in accordance with paragraph (3), other joint cross-border initiatives already take place within the region in which the IBET would be established, including other Department cross-border programs such as the Integrated Cross-Border Maritime Law Enforcement Operation Program established under section 711 of the Coast Guard and Maritime Transportation Act of 2012 (46 U.S.C. 70101 note) or the Border Enforcement Security Task Force established under section 432.

“(3) DUPLICATION OF EFFORTS.—In determining whether to establish a new IBET or to expand an existing IBET in a given region, the Secretary shall ensure that the IBET under consideration does not duplicate the efforts of other existing interagency task forces or centers within such region, including the Integrated Cross-Border Maritime Law Enforcement Operation Program established under section 711 of the Coast Guard and Maritime Transportation Act of 2012 (46 U.S.C. 70101 note) or the Border Enforcement Security Task Force established under section 432.

“(d) OPERATION.—
“(1) IN GENERAL.—After determining the regions in which to establish IBETs, the Secretary may—

“(A) direct the assignment of Federal personnel to such IBETs; and

“(B) take other actions to assist Federal, State, local, and tribal entities to participate in such IBETs, including providing financial assistance, as appropriate, for operational, administrative, and technological costs associated with such participation.

“(2) LIMITATION.—Coast Guard personnel assigned under paragraph (1) may be assigned only for the purposes of securing the maritime borders of the United States, in accordance with subsection (e)(1)(C).

“(e) COORDINATION.—The Secretary shall coordinate the IBET program with other similar border security and antiterrorism programs within the Department in accordance with the strategic objectives of the Cross-Border Law Enforcement Advisory Committee.

“(f) MEMORANDA OF UNDERSTANDING.—The Secretary may enter into memoranda of understanding with appropriate representatives of the entities specified in subsection (e)(1) necessary to carry out the IBET program.
“(g) REPORT.—Not later than 180 days after the date on which an IBET is established and biannually thereafter for the following six years, the Secretary shall submit to the appropriate congressional committees, including the Committee on Homeland Security of the House of Representatives and the Committee on Homeland Security and Governmental Affairs of the Senate, and in the case of Coast Guard personnel used to secure the maritime borders of the United States, additionally to the Committee on Transportation and Infrastructure of the House of Representatives, a report that—

“(1) describes the effectiveness of IBETs in fulfilling the purposes specified in subsection (b);

“(2) assesses the impact of certain challenges on the sustainment of cross-border IBET operations, including challenges faced by international partners;

“(3) addresses ways to support joint training for IBET stakeholder agencies and radio interoperability to allow for secure cross-border radio communications; and

“(4) assesses how IBETs, Border Enforcement Security Task Forces, and the Integrated Cross-Border Maritime Law Enforcement Operation Program can better align operations, including interdiction and investigation activities.”.
(b) CLERICAL AMENDMENT.—The table of contents in section 1(b) of the Homeland Security Act of 2002 is amended by adding after the item relating to section 419 the following new item:

“Sec. 420. Immigration cooperation program.
“Sec. 420A. Air cargo advance screening.
“Sec. 420B. U.S. Customs and Border Protection Office of Air and Marine Operations asset deployment.
“Sec. 420C. Integrated Border Enforcement Teams.”.

(c) DEADLINE FOR AIR CARGO ADVANCE SCREENING.—The Commissioner of U.S. Customs and Border Protection shall implement section 420A of the Homeland Security Act of 2002, as added by this section, by not later than one year after the date of the enactment of this Act.

SEC. 202. BORDER AND MARITIME SECURITY EFFICIENCIES.

(a) IN GENERAL.—Subtitle C of title IV of the Homeland Security Act of 2002 (6 U.S.C. 231 et seq.) is amended by adding at the end the following new sections:

“SEC. 434. BORDER SECURITY JOINT TASK FORCES.

“(a) ESTABLISHMENT.—The Secretary shall establish and operate the following departmental Joint Task Forces (in this section referred to as ‘Joint Task Force’) to conduct joint operations using Department component and office personnel and capabilities to secure the land and maritime borders of the United States:
“(1) JOINT TASK FORCE—EAST.—Joint Task Force—East shall, at the direction of the Secretary and in coordination with Joint Task Force—West, create and execute a strategic plan to secure the land and maritime borders of the United States and shall operate and be located in a place or region determined by the Secretary.

“(2) JOINT TASK FORCE—WEST.—Joint Task Force—West shall, at the direction of the Secretary and in coordination with Joint Task Force—East, create and execute a strategic plan to secure the land and maritime borders of the United States and shall operate and be located in a place or region determined by the Secretary.

“(3) JOINT TASK FORCE—INVESTIGATIONS.—Joint Task Force—Investigations shall, at the direction of the Secretary, be responsible for coordinating criminal investigations supporting Joint Task Force—West and Joint Task Force—East.

“(b) JOINT TASK FORCE DIRECTORS.—The Secretary shall appoint a Director to head each Joint Task Force. Each Director shall be a senior official selected from a relevant component or office of the Department, rotating between relevant components and offices every two years. The Secretary may extend the appointment of
a Director for up to two additional years, if the Secretary
determines that such an extension is in the best interest
of the Department.

“(c) Initial Appointments.—The Secretary shall
make the following appointments to the following Joint
Task Forces:

“(1) The initial Director of Joint Task Force–
East shall be a senior officer of the Coast Guard.

“(2) The initial Director of Joint Task Force–
West shall be a senior official of U.S. Customs and
Border Protection.

“(3) The initial Director of Joint Task Force–
Investigations shall be a senior official of U.S. Immi-
gration and Customs Enforcement.

“(d) Joint Task Force Deputy Directors.—The
Secretary shall appoint a Deputy Director for each Joint
Task Force. The Deputy Director of a Joint Task Force
shall, to the greatest extent practicable, be an official of
a different component or office than the Director of each
Joint Task Force.

“(e) Responsibilities.—Each Joint Task Force Di-
rector shall—

“(1) identify and prioritize border and maritime
security threats to the homeland;
“(2) maintain situational awareness within their areas of responsibility, as determined by the Secretary;

“(3) provide operational plans and requirements for standard operating procedures and contingency operations;

“(4) plan and execute joint task force activities within their areas of responsibility, as determined by the Secretary;

“(5) set and accomplish strategic objectives through integrated operational planning and execution;

“(6) exercise operational direction over personnel and equipment from Department components and offices allocated to the respective Joint Task Force to accomplish task force objectives;

“(7) establish operational and investigative priorities within the Director’s operating areas;

“(8) coordinate with foreign governments and other Federal, State, and local agencies, where appropriate, to carry out the mission of the Director’s Joint Task Force;

“(9) identify and provide to the Secretary the joint mission requirements necessary to secure the land and maritime borders of the United States; and
“(10) carry out other duties and powers the Secretary determines appropriate.

“(f) PERSONNEL AND RESOURCES OF JOINT TASK FORCES.—

“(1) IN GENERAL.—The Secretary may, upon request of the Director of a Joint Task Force, allocate on a temporary basis component and office personnel and equipment to the requesting Joint Task Force, with appropriate consideration of risk given to the other primary missions of the Department.

“(2) CONSIDERATION OF IMPACT.—When reviewing requests for allocation of component personnel and equipment under paragraph (1), the Secretary shall consider the impact of such allocation on the ability of the donating component to carry out the primary missions of the Department, and in the case of the Coast Guard, the missions specified in section 888.

“(3) LIMITATION.—Personnel and equipment of the Coast Guard allocated under this subsection may only be used to carry out operations and investigations related to securing the maritime borders of the United States.

“(g) COMPONENT RESOURCE AUTHORITY.—As directed by the Secretary—
“(1) each Director of a Joint Task Force shall be provided sufficient resources from relevant components and offices of the Department and the authority necessary to carry out the missions and responsibilities required under this section;

“(2) the resources referred to in paragraph (1) shall be under the operational authority, direction, and control of the Director of the Joint Task Force to which such resources were assigned; and

“(3) the personnel and equipment of the Joint Task Forces shall remain under the administrative direction of its primary component or office.

“(h) JOINT TASK FORCE STAFF.—Each Joint Task Force shall have a staff to assist the Directors in carrying out the mission and responsibilities of the Joint Task Forces. Such staff shall be filled by officials from relevant components and offices of the Department.

“(i) ESTABLISHMENT OF PERFORMANCE METRICS.—The Secretary shall—

“(1) establish performance metrics to evaluate the effectiveness of the Joint Task Forces in securing the land and maritime borders of the United States;

“(2) submit such metrics to the Committee on Homeland Security of the House of Representatives
and the Committee on Homeland Security and Governmental Affairs of the Senate, and in the case of metrics related to securing the maritime borders of the United States, additionally to the Committee on Transportation and Infrastructure of the House of Representatives, by the date that is not later than 120 days after the date of the enactment of this section; and

“(3) submit to such Committees—

“(A) an initial report that contains the evaluation described in paragraph (1) by not later than January 31, 2017; and

“(B) a second report that contains such evaluation by not later than January 31, 2018.

“(j) JOINT DUTY TRAINING PROGRAM.—

“(1) IN GENERAL.—The Secretary shall establish a Department joint duty training program for the purposes of enhancing departmental unity of efforts and promoting workforce professional development. Such training shall be tailored to improve joint operations as part of the Joint Task Forces established under subsection (a).

“(2) ELEMENTS.—The joint duty training program established under paragraph (1) shall address, at minimum, the following topics:
“(A) National strategy.

“(B) Strategic and contingency planning.

“(C) Command and control of operations under joint command.

“(D) International engagement.


“(F) Border security.

“(G) Interagency collaboration.

“(H) Leadership.

“(3) Officers and officials.—The joint duty training program established under paragraph (1) shall consist of—

“(A) one course intended for mid-level officers and officials of the Department assigned to or working with the Joint Task Forces, and

“(B) one course intended for senior officers and officials of the Department assigned to or working with the Joint Task Forces, to ensure a systematic, progressive, and career-long development of such officers and officials in coordinating and executing Department-wide joint planning and operations.

“(4) Training required.—

“(A) Directors and deputy directors.—Except as provided in subparagraph

•HR 6381 IH
(C), each Joint Task Force Director and Deputy Director of a Joint Task Force shall complete relevant parts of the joint duty training program under this subsection prior to assignment to a Joint Task Force.

“(B) JOINT TASK FORCE STAFF.—All senior and mid-level officers and officials serving on the staff of a Joint Task Force shall complete relevant parts of the joint duty training program under this subsection within the first year of assignment to a Joint Task Force.

“(C) EXCEPTION.—Subparagraph (A) does not apply in the case of the initial Directors and Deputy Directors of a Joint Task Force.

“(k) ESTABLISHING ADDITIONAL JOINT TASK FORCES.—The Secretary may establish additional Joint Task Forces for the purposes of—

“(1) coordinating operations along the northern border of the United States;

“(2) homeland security crises, subject to subsection (l);

“(3) establishing other regionally based operations; or

“(4) cybersecurity.
“(l) LIMITATION ON ADDITIONAL JOINT TASK FORCES.—

“(1) IN GENERAL.—The Secretary may not establish a Joint Task Force for any major disaster or emergency declared under the Robert T. Stafford Disaster Relief and Emergency Assistance Act (42 U.S.C. 5121 et seq.) or an incident for which the Federal Emergency Management Agency has primary responsibility for management of the response under title V of this Act, including section 504(a)(3)(A), unless the responsibilities of the Joint Task Force—

“(A) do not include operational functions related to incident management, including coordination of operations; and

“(B) are consistent with the requirements of sections 509(c), 503(c)(3), and 503(c)(4)(A) of this Act and section 302 of the Robert T. Stafford Disaster Relief and Emergency Assistance Act (42 U.S.C. 5143).

“(2) RESPONSIBILITIES AND FUNCTIONS NOT REDUCED.—Nothing in this section reduces the responsibilities or functions of the Federal Emergency Management Agency or the Administrator of the Federal Emergency Management Agency under title
V of this Act, provisions of law enacted by the Post-Katrina Emergency Management Reform Act of 2006 (Public Law 109–295), and other laws, including the diversion of any asset, function, or mission from the Federal Emergency Management Agency or the Administrator of the Federal Emergency Management Agency pursuant to section 506.

“(m) NOTIFICATION.—

“(1) IN GENERAL.—The Secretary shall submit a notification to the Committee on Homeland Security of the House of Representatives and the Committee on Homeland Security and Governmental Affairs of the Senate, and in the case of a Joint Task Force in which the Coast Guard will participate or a Joint Task Force established under paragraph (2) or (3) of subsection (k) to the Committee on Transportation and Infrastructure of the House of Representatives, 90 days prior to the establishment of the Joint Task Force.

“(2) WAIVER AUTHORITY.—The Secretary may waive the requirement of paragraph (1) in the event of an emergency circumstance that imminently threatens the protection of human life or the protection of property.

“(n) REVIEW.—
“(1) IN GENERAL.—The Inspector General of the Department shall conduct a review of the Joint Task Forces established under this section.

“(2) CONTENTS.—The review required under paragraph (1) shall include an assessment of the effectiveness of the Joint Task Force structure in securing the land and maritime borders of the United States, together with recommendations for enhancements to such structure to further strengthen border security.

“(3) SUBMISSION.—The Inspector General of the Department shall submit to the Committee on Homeland Security and the Committee on Transportation and Infrastructure of the House of Representatives and the Committee on Homeland Security and Governmental Affairs of the Senate a report that contains the review required under paragraph (1) by not later than January 31, 2018.

“(o) DEFINITION.—In this section, the term ‘situational awareness’ means a knowledge and unified understanding of unlawful cross-border activity, including threats and trends concerning illicit trafficking and unlawful crossings, and the ability to forecast future shifts in such threats and trends, the ability to evaluate such threats and trends at a level sufficient to create actionable

•HR 6381 IH
plans, and the operational capability to conduct continuous and integrated surveillance of the land and maritime borders of the United States.

“(p) SUNSET.—This section expires on September 30, 2018.

“SEC. 435. UPDATES OF MARITIME OPERATIONS COORDINATION PLAN.

“(a) IN GENERAL.—Not later than 180 days after the enactment of this section, the Secretary shall submit to the Committee on Homeland Security and the Committee on Transportation and Infrastructure of the House of Representatives and the Committee on Homeland Security and Governmental Affairs of the Senate a maritime operations coordination plan for the coordination and cooperation of maritime operations undertaken by components and offices of the Department with responsibility for maritime security missions. Such plan shall update the maritime operations coordination plan released by the Department in July 2011, and shall address the following:

“(1) Coordination of planning, integration of maritime operations, and development of joint maritime domain awareness efforts of any component or office of the Department with responsibility for maritime homeland security missions.
“(2) Maintaining effective information sharing and, as appropriate, intelligence integration, with Federal, State, and local officials and the private sector, regarding threats to maritime security.

“(3) Leveraging existing departmental coordination mechanisms, including the interagency operational centers as authorized under section 70107A of title 46, United States Code, Coast Guard’s Regional Coordinating Mechanisms, the U.S. Customs and Border Protection Air and Marine Operations Center, the U.S. Customs and Border Protection Operational Integration Center, and other regional maritime operational command centers.

“(4) Cooperation and coordination with other departments and agencies of the Federal Government, and State and local agencies, in the maritime environment, in support of maritime homeland security missions.

“(5) Work conducted within the context of other national and Department maritime security strategic guidance.

“(b) ADDITIONAL UPDATES.—Not later than July 1, 2020, the Secretary, acting through the Department’s Office of Operations Coordination and Planning, shall submit to the Committee on Homeland Security and the Com-
mittee on Transportation and Infrastructure of the House of Representatives and the Committee on Homeland Security and Governmental Affairs of the Senate an update to the maritime operations coordination plan required under subsection (a).”.

(b) Clerical Amendment.—The table of contents in section 1(b) of the Homeland Security Act of 2002 is amended by adding after the item relating to section 433 the following new items:

“Sec. 435. Updates of maritime operations coordination plan.”.

SEC. 203. PUBLIC-PRIVATE PARTNERSHIPS.

(a) In General.—Title IV of the Homeland Security Act of 2002 (6 U.S.C. 201 et seq.) is amended by adding at the end the following new subtitle:

“Subtitle G—U.S. Customs and Border Protection Public Private Partnerships

SEC. 481. FEE AGREEMENTS FOR CERTAIN SERVICES AT PORTS OF ENTRY.

“(a) In General.—Notwithstanding section 13031(e) of the Consolidated Omnibus Budget Reconciliation Act of 1985 (19 U.S.C. 58c(e)) and section 451 of the Tariff Act of 1930 (19 U.S.C. 1451), the Commissioner of U.S. Customs and Border Protection may, upon
the request of any entity, enter into a fee agreement with
such entity under which—

“(1) U.S. Customs and Border Protection shall
provide services described in subsection (e) at a
United States port of entry or any other facility at
which U.S. Customs and Border Protection provides
or will provide such services;

“(2) such entity shall remit to U.S. Customs
and Border Protection a fee imposed under sub-
section (e) in an amount equal to the full costs that
are incurred or will be incurred in providing such
services; and

“(3) if space is provided by such entity, each
facility at which U.S. Customs and Border Protec-
tion services are performed shall be maintained and
equipped by such entity, without cost to the Federal
Government, in accordance with U.S. Customs and
Border Protection specifications.

“(b) SERVICES DESCRIBED.—The services described
in this section are any activities of any employee or con-
tractor of U.S. Customs and Border Protection pertaining
to, or in support of, customs, agricultural processing, bor-
der security, or immigration inspection-related matters at
a port of entry or any other facility at which U.S. Customs
and Border Protection provides or will provide services.
“(c) LIMITATIONS.—

“(1) IMPACTS OF SERVICES.—The Commissioner of U.S. Customs and Border Protection—

“(A) may enter into fee agreements under this section only for services that will increase or enhance the operational capacity of U.S. Customs and Border Protection based on available staffing and workload and that will not shift the cost of services funded in any appropriations Act, or provided from any account in the Treasury of the United States derived by the collection of fees, to entities under this Act; and

“(B) may not enter into a fee agreement under this section if such agreement would un- duly and permanently impact services funded in any appropriations Act, or provided from any account in the Treasury of the United States, derived by the collection of fees.

“(2) NUMBER.—There shall be no limit to the number of fee agreements that the Commissioner of U.S. Customs and Border Protection may enter into under this section.

“(d) FEE.—
“(1) IN GENERAL.—The amount of the fee to be charged pursuant to an agreement authorized under subsection (a) shall be paid by each entity requesting U.S. Customs and Border Protection services, and shall be for the full cost of providing such services, including the salaries and expenses of employees and contractors of U.S. Customs and Border Protection, to provide such services and other costs incurred by U.S. Customs and Border Protection relating to such services, such as temporary placement or permanent relocation of such employees and contractors.

“(2) TIMING.—The Commissioner of U.S. Customs and Border Protection may require that the fee referred to in paragraph (1) be paid by each entity that has entered into a fee agreement under subsection (a) with U.S. Customs and Border Protection in advance of the performance of U.S. Customs and Border Protection services.

“(3) OVERSIGHT OF FEES.—The Commissioner of U.S. Customs and Border Protection shall develop a process to oversee the services for which fees are charged pursuant to an agreement under subsection (a), including the following:
“(A) A determination and report on the full costs of providing such services, as well as a process for increasing such fees, as necessary.

“(B) Establishment of a periodic remittance schedule to replenish appropriations, accounts, or funds, as necessary.

“(C) Identification of costs paid by such fees.

“(e) DEPOSIT OF FUNDS.—

“(1) ACCOUNT.—Funds collected pursuant to any agreement entered into under subsection (a) shall be deposited as offsetting collections, shall remain available until expended without fiscal year limitation, and shall be credited to the applicable appropriation, account, or fund for the amount paid out of such appropriation, account, or fund for any expenses incurred or to be incurred by U.S. Customs and Border Protection in providing U.S. Customs and Border Protection services under any such agreement and any other costs incurred or to be incurred by U.S. Customs and Border Protection relating to such services.

“(2) RETURN OF UNUSED FUNDS.—The Commissioner of U.S. Customs and Border Protection shall return any unused funds collected and depos-
ited into the account described in paragraph (1) in
the event that a fee agreement entered into under
subsection (a) is terminated for any reason, or in the
event that the terms of such fee agreement change
by mutual agreement to cause a reduction of U.S.
Customs and Border Protections services. No inter-
est shall be owed upon the return of any such un-
used funds.

“(f) TERMINATION.—

“(1) IN GENERAL.—The Commissioner of U.S.
Customs and Border Protection shall terminate the
provision of services pursuant to a fee agreement en-
tered into under subsection (a) with an entity that,
after receiving notice from the Commissioner that a
fee under subsection (d) is due, fails to pay such fee
in a timely manner. In the event of such termi-
nation, all costs incurred by U.S. Customs and Bor-
der Protection which have not been paid shall be-
come immediately due and payable. Interest on un-
paid fees shall accrue based on the rate and amount
established under sections 6621 and 6622 of the In-

“(2) PENALTY.—Any entity that, after notice
and demand for payment of any fee under sub-
section (d), fails to pay such fee in a timely manner
shall be liable for a penalty or liquidated damage equal to two times the amount of such fee. Any such amount collected pursuant to this paragraph shall be deposited into the appropriate account specified under subsection (e) and shall be available as described in such subsection.

“(g) ANNUAL REPORT.—The Commissioner of U.S. Customs and Border Protection shall submit to the Committee on Homeland Security, the Committee on Appropriations, and the Committee on Ways and Means of the House of Representatives and the Committee on Homeland Security and Governmental Affairs, the Committee on Appropriations, and the Committee on Finance of the Senate an annual report identifying the activities undertaken and the agreements entered into pursuant to this section.

“(h) RULE OF CONSTRUCTION.—Nothing in this section may be construed as imposing in any manner on U.S. Customs and Border Protection any responsibilities, duties, or authorities relating to real property.

“SEC. 482. PORT OF ENTRY DONATION AUTHORITY.

“(a) PERSONAL PROPERTY DONATION AUTHORITY.—

“(1) IN GENERAL.—The Commissioner of U.S. Customs and Border Protection, in consultation with
the Administrator of General Services, may enter
into an agreement with any entity to accept a dona-
tion of personal property, money, or nonpersonal
services for uses described in paragraph (3) only
with respect to the following locations at which U.S.
Customs and Border Protection performs or will be
performing inspection services:

“(A) A new or existing sea or air port of
entry.

“(B) An existing Federal Government-
owned land port of entry.

“(C) A new Federal Government-owned
land port of entry if—

“(i) the fair market value of the dona-
tion is $50,000,000 or less; and

“(ii) the fair market value, including
any personal and real property donations
in total, of such port of entry when com-
pleted, is $50,000,000 or less.

“(2) LIMITATION ON MONETARY DONATIONS.—
Any monetary donation accepted pursuant to this
subsection may not be used to pay the salaries of
U.S. Customs and Border Protection employees per-
forming inspection services.
“(3) USE.—Donations accepted pursuant to this subsection may be used for activities related to a new or existing sea or air port of entry or a new or existing Federal Government-owned land port of entry described in paragraph (1), including expenses related to—

“(A) furniture, fixtures, equipment, or technology, including installation or the deployment thereof; and

“(B) operation and maintenance of such furniture, fixtures, equipment, or technology.

“(b) REAL PROPERTY DONATION AUTHORITY.—

“(1) IN GENERAL.—Subject to paragraph (3), the Commissioner of U.S. Customs and Border Protection, and the Administrator of the General Services Administration, as applicable, may enter into an agreement with any entity to accept a donation of real property or money for uses described in paragraph (2) only with respect to the following locations at which U.S. Customs and Border Protection performs or will be performing inspection services:

“(A) A new or existing sea or air port of entry.

“(B) An existing Federal Government-owned land port of entry.
“(C) A new Federal Government-owned land port of entry if—

“(i) the fair market value of the donation is $50,000,000 or less; and

“(ii) the fair market value, including any personal and real property donations in total, of such port of entry when completed, is $50,000,000 or less.

“(2) USE.—Donations accepted pursuant to this subsection may be used for activities related to construction, alteration, operation, or maintenance of a new or existing sea or air port of entry or a new or existing a Federal Government-owned land port of entry described in paragraph (1), including expenses related to—

“(A) land acquisition, design, construction, repair, or alteration; and

“(B) operation and maintenance of such port of entry facility.

“(3) LIMITATION ON REAL PROPERTY DONATIONS.—A donation of real property under this subsection at an existing land port of entry owned by the General Services Administration may only be accepted by the Administrator of General Services.

“(4) SUNSET.—
“(A) IN GENERAL.—The authority to enter into an agreement under this subsection shall terminate on the date that is five years after the date of the enactment of this subsection.

“(B) RULE OF CONSTRUCTION.—The termination date referred to in subparagraph (A) shall not apply to carrying out the terms of an agreement under this subsection if such agreement is entered into before such termination date.

“(c) GENERAL PROVISIONS.—

“(1) DURATION.—An agreement entered into under subsection (a) or (b) (and, in the case of such subsection (b), in accordance with paragraph (4) of such subsection) may last as long as required to meet the terms of such agreement.

“(2) CRITERIA.—In carrying out agreements entered into under subsection (a) or (b), the Commissioner of U.S. Customs and Border Protection, in consultation with the Administrator of General Services, shall establish criteria that includes the following:

“(A) Selection and evaluation of donors.

“(B) Identification of roles and responsibilities between U.S. Customs and Border Protec-
tion, the General Services Administration, as applicable, and donors.

“(C) Identification, allocation, and management of explicit and implicit risks of partnering between the Federal Government and donors.

“(D) Decisionmaking and dispute resolution processes.

“(E) Processes for U.S. Customs and Border Protection, and the General Services Administration, as applicable, to terminate agreements if selected donors are not meeting the terms of any such agreement, including the security standards established by U.S. Customs and Border Protection.

“(3) EVALUATION PROCEDURES.—

“(A) IN GENERAL.—The Commissioner of U.S. Customs and Border Protection, in consultation with the Administrator of General Services, as applicable, shall—

“(i) establish criteria for evaluating a proposal to enter into an agreement under subsection (a) or (b); and

“(ii) make such criteria publicly available.
“(B) CONSIDERATIONS.—Criteria established pursuant to subparagraph (A) shall consider the following:

“(i) The impact of a proposal referred to in such subparagraph on the land, sea, or air port of entry at issue and other ports of entry or similar facilities or other infrastructure near the location of the proposed donation.

“(ii) Such proposal’s potential to increase trade and travel efficiency through added capacity.

“(iii) Such proposal’s potential to enhance the security of the port of entry at issue.

“(iv) For a donation under subsection (b)—

“(I) whether such donation satisfies the requirements of such proposal, or whether additional real property would be required; and

“(II) an explanation of how such donation was acquired, including if eminent domain was used.
“(v) The funding available to complete
the intended use of such donation.

“(vi) The costs of maintaining and
operating such donation.

“(vii) The impact of such proposal on
U.S. Customs and Border Protection staff-
ing requirements.

“(viii) Other factors that the Commis-
sioner or Administrator determines to be
relevant.

“(C) DETERMINATION AND NOTIFI-
CATION.—Not later than 180 days after receiving
a proposal to enter into an agreement under
subsection (a) or (b), the Commissioner of U.S.
Customs and Border Protection, with the con-
currence of the Administrator of General Serv-
ices, as applicable, shall make a determination
to deny or approve such proposal, and shall no-
tify the entity that submitted such proposal of
such determination.

“(4) SUPPLEMENTAL FUNDING.—Except as re-
quired under section 3307 of title 40, United States
Code, for real property donations to the Adminis-
trator of General Services at a GSA-owned land port
of entry, donations made pursuant to subsection (a)
and (b) may be used in addition to any other funding for such purpose, including appropriated funds, property, or services.

“(5) RETURN OF DONATIONS.—The Commissioner of U.S. Customs and Border Protection, or the Administrator of General Services, as applicable, may return any donation made pursuant to subsection (a) or (b). No interest shall be owed to the donor with respect to any donation provided under such subsections that is returned pursuant to this subsection.

“(6) PROHIBITION ON CERTAIN FUNDING.—Except as provided in subsections (a) and (b) regarding the acceptance of donations, the Commissioner of U.S. Customs and Border Protection and the Administrator of General Services, as applicable, may not, with respect to an agreement entered into under either of such subsections, obligate or expend amounts in excess of amounts that have been appropriated pursuant to any appropriations Act for purposes specified in either of such subsections or otherwise made available for any of such purposes.

“(7) ANNUAL REPORTS.—The Commissioner of U.S. Customs and Border Protection, in collaboration with the Administrator of General Services, as
applicable, shall submit to the Committee on Homeland Security, the Committee on Transportation and Infrastructure, and the Committee on Appropriations of the House of Representatives and the Committee on Homeland Security and Governmental Affairs, the Committee on Environment and Public Works, and the Committee on Appropriations of the Senate an annual report identifying the activities undertaken and agreements entered into pursuant to subsections (a) and (b).

“(d) Rule of Construction.—Except as otherwise provided in this section, nothing in this section may be construed as affecting in any manner the responsibilities, duties, or authorities of U.S. Customs and Border Protection or the General Services Administration.


“Nothing in this subtitle may be construed as affecting in any manner—

“(1) any agreement entered into pursuant to section 560 of division D of the Consolidated and Further Continuing Appropriations Act, 2013 (Public Law 113–6) or section 559 of title V of division F of the Consolidated Appropriations Act, 2014 (6 U.S.C. 211 note; Public Law 113–76), as in existence on the day before the date of the enactment of
this subtitle, and any such agreement shall continue to have full force and effect on and after such date; or

“(2) a proposal accepted for consideration by U.S. Customs and Border Protection pursuant to such section 559, as in existence on the day before such date of enactment.

“SEC. 484. DEFINITIONS.

“In this subtitle:

“(1) DONOR.—The term ‘donor’ means any entity that is proposing to make a donation under this Act.

“(2) ENTITY.—The term ‘entity’ means any—

“(A) person;

“(B) partnership, corporation, trust, estate, cooperative, association, or any other organized group of persons;

“(C) Federal, State or local government (including any subdivision, agency or instrumentality thereof); or

“(D) any other private or governmental entity.”.

(b) CLERICAL AMENDMENT.—The table of contents in section 1(b) of the Homeland Security Act of 2002 is
amended by adding at the end of the list of items relating
to title IV the following new items:

“Subtitle G—U.S. Customs and Border Protection Public Private
Partnerships

“Sec. 481. Fee agreements for certain services at ports of entry.
“Sec. 482. Port of entry donation authority.
“Sec. 483. Current and proposed agreements.
“Sec. 484. Definitions.”.

(c) REPEALS.—Section 560 of division D of the Con-
solidated and Further Continuing Appropriations Act,
2013 (Public Law 113–6) and section 559 of title V of
division F of the Consolidated Appropriations Act, 2014
(6 U.S.C. 211 note; Public Law 113–76) are repealed.

SEC. 204. ESTABLISHMENT OF THE OFFICE OF BIOMETRIC
IDENTITY MANAGEMENT.

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

“SEC. 708. OFFICE OF BIOMETRIC IDENTITY MANAGEMENT.

“(a) ESTABLISHMENT.—The Office of Biometric
Identity Management is established within the Depart-
ment.

“(b) DIRECTOR.—

“(1) IN GENERAL.—The Office of Biometric
Identity Management shall be administered by the
Director of the Office of Biometric Identity Manage-
ment (in this section referred to as the ‘Director’)

•HR 6381 IH
who shall report to the Secretary, or to another official of the Department, as the Secretary may direct.

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

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

“(B) lead the Department’s biometric identity services to support anti-terrorism, counter-terrorism, border security, credentialing, national security, and public safety and enable operational missions across the Department by matching, storing, sharing, and analyzing biometric data;

“(C) deliver biometric identity information and analysis capabilities to—

“(i) the Department and its components;

“(ii) appropriate Federal, State, local, and tribal agencies;

“(iii) appropriate foreign governments; and

“(iv) appropriate private sector entities;
“(D) support the law enforcement, public safety, national security, and homeland security missions of other Federal, State, local, and tribal agencies, as appropriate;

“(E) establish and manage the operation and maintenance of the Department’s sole biometric repository;

“(F) establish, manage, and operate Biometric Support Centers to provide biometric identification and verification analysis and services to the Department, appropriate Federal, State, local, and tribal agencies, appropriate foreign governments, and appropriate private sector entities;

“(G) in collaboration with the Undersecretary for Science and Technology, establish a Department-wide research and development program to support efforts in assessment, development, and exploration of biometric advancements and emerging technologies;

“(H) oversee Department-wide standards for biometric conformity, and work to make such standards Government-wide;

“(I) in coordination with the Department’s Office of Policy, and in consultation with rel-
evant component offices and headquarters offices, enter into data sharing agreements with appropriate Federal agencies to support immigration, law enforcement, national security, and public safety missions;

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

“(K) carry out the duties and powers prescribed by law or delegated by the Secretary.

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

“(d) CHIEF TECHNOLOGY OFFICER.—

“(1) IN GENERAL.—There shall be in the Office of Biometric Identity Management a Chief Technology Officer.

“(2) DUTIES.—The Chief Technology Officer shall—

“(A) ensure compliance with policies, processes, standards, guidelines, and procedures related to information technology systems management, enterprise architecture, and data management;
“(B) provide engineering and enterprise architecture guidance and direction to the Office of Biometric Identity Management; and

“(C) leverage emerging biometric technologies to recommend improvements to major enterprise applications, identify tools to optimize information technology systems performance, and develop and promote joint technology solutions to improve services to enhance mission effectiveness.

“(e) Other Authorities.—

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

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

(b) Transfer Limitation.—The Secretary of Homeland Security may not transfer the location or re-
porting structure of the Office of Biometric Identity Management (established by section 708 of the Homeland Security Act of 2002, as added by subsection (a) of this section) to any component of the Department of Homeland Security.

(c) Clerical Amendment.—The table of contents in section 1(b) of the Homeland Security Act of 2002 is amended by adding after the item relating to section 707 the following new item:

“Sec. 708. Office of Biometric Identity Management.”.

SEC. 205. COST-BENEFIT ANALYSIS OF CO-LOCATING OPERATIONAL ENTITIES.

(a) In General.—For any location in which U.S. Customs and Border Protection’s Office of Air and Marine Operations is based within 45 miles of locations where any other Department of Homeland Security agency also operates air and marine assets, the Secretary of Homeland Security shall conduct a cost-benefit analysis to consider the potential cost of and savings derived from co-locating aviation and maritime operational assets of the respective agencies of the Department. In analyzing such potential cost savings achieved by sharing aviation and maritime facilities, such analysis shall consider, at a minimum, the following factors:

(1) Potential enhanced cooperation derived from Department personnel being co-located.
(2) Potential costs of, and savings derived through, shared maintenance and logistics facilities and activities.

(3) Joint use of base and facility infrastructure, such as runways, hangars, control towers, operations centers, piers and docks, boathouses, and fuel depots.

(4) Potential operational costs of co-locating aviation and maritime assets and personnel.

(5) Short term moving costs required in order to co-locate facilities.

(6) Acquisition and infrastructure costs for enlarging current facilities, as needed.

(b) REPORT.—Not later than one year after the date of the enactment of this Act, the Secretary of Homeland Security shall submit to the Committee on Homeland Security and the Committee on Transportation and Infrastructure of the House of Representatives and the Committee on Homeland Security and Governmental Affairs of the Senate a report summarizing the results of the cost-benefit analysis required under subsection (a) and any planned actions based upon such results.
SEC. 206. STRATEGIC PERSONNEL PLAN FOR U.S. CUSTOMS AND BORDER PROTECTION PERSONNEL DEPLOYED ABROAD.

(a) IN GENERAL.—Not later than 270 days of after the date of the enactment of this Act, the Commissioner of U.S. Customs and Border Protection shall provide to the Committee on Homeland Security of the House of Representatives and the Committee on Homeland Security and Governmental Affairs of the Senate a three year strategic plan for deployment of U.S. Customs and Border Protection (in this section referred to as “CBP”) personnel to locations outside the United States.

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

(1) A risk-based method for determining expansion of CBP international programs to new locations, given resource constraints.

(2) A plan to ensure CBP personnel deployed at locations outside the United States have appropriate oversight and support to ensure performance in support of program goals.

(3) Information on planned future deployments of CBP personnel for a three year period, together with corresponding information on locations for such deployments outside the United States.
(c) CONSIDERATIONS.—In preparing the plan required under subsection (a), the Commissioner of U.S. Customs and Border Protection shall consider, and include information on, the following:

(1) Existing CBP programs in operation outside of the United States, together with specific information on locations outside the United States in which each such program operates.

(2) The number of CBP personnel deployed at each location outside the United States during the preceding fiscal year.

SEC. 207. THREAT ASSESSMENT FOR UNITED STATES-BOUND INTERNATIONAL MAIL.

Not later than 180 days after the date of the enactment of this Act, the Commissioner of U.S. Customs and Border Protection shall submit to the Committee on Homeland Security of the House of Representatives and the Committee on Homeland Security and Governmental Affairs of the Senate an assessment of the security threats posed by United States-bound international mail.

SEC. 208. EVALUATION OF COAST GUARD DEPLOYABLE SPECIALIZED FORCES.

(a) IN GENERAL.—Not later than one year after the date of the enactment of this Act, the Comptroller General of the United States shall submit to the Committee on
Homeland Security and the Committee on Transportation and Infrastructure of the House of Representatives and the Committee on Homeland Security and Governmental Affairs and the Committee on Commerce, Science, and Transportation of the Senate a report that describes and assesses the state of the Coast Guard’s Deployable Specialized Forces (in this section referred to as the “DSF”).

Such report shall include, at a minimum, the following elements:

(1) For each of the past three fiscal years, and for each type of DSF, the following:

(A) A cost analysis, including training, operating, and travel costs.

(B) The number of personnel assigned.

(C) The total number of units.

(D) The total number of operations conducted.

(E) The number of operations requested by each of the following:

(i) The Coast Guard.

(ii) Other components or offices of the Department of Homeland Security.

(iii) Other Federal departments or agencies.

(iv) State agencies.
(v) Local agencies.

(F) The number of operations fulfilled by the entities specified in subparagraph (E).

(2) Mission impact, feasibility, and cost, including potential cost savings, of locating DSF capabilities, including the following scenarios:

(A) Combining DSFs, primarily focused on counterdrug operations, under one centralized command.

(B) Distributing counter-terrorism and anti-terrorism capabilities to DSFs in each major United States port.

(b) DEPLOYABLE SPECIALIZED FORCE DEFINED.—In this section, the term “Deployable Specialized Force” means a unit of the Coast Guard that serves as a quick reaction force designed to be deployed to handle counterdrug, counter-terrorism, and anti-terrorism operations or other maritime threats to the United States.

SEC. 209. CUSTOMS-TRADE PARTNERSHIP AGAINST TERRORISM IMPROVEMENT.

(b) Recognition of Other Countries’ Trusted Shipper Programs.—

(1) In general.—Section 218 of the Security and Accountability for Every Port Act of 2006 (6 U.S.C. 968) is amended to read as follows:

“SEC. 218. RECOGNITION OF OTHER COUNTRIES’ TRUSTED SHIPPER PROGRAMS.

“Not later than 30 days before signing an arrangement between the United States and a foreign government providing for mutual recognition of supply chain security practices which might result in the utilization of benefits described in section 214, 215, or 216, the Secretary shall—

“(1) notify the appropriate congressional committees of the proposed terms of such arrangement; and

“(2) determine, in consultation with the Commissioner, that such foreign government’s supply chain security program provides comparable security as that provided by C–TPAT.”.

(2) Clerical amendment.—The table of contents in section 1(b) of the Security and Accountability for Every Port Act of 2006 is amended by amending the item relating to section 218 to read as follows:

“Sec. 218. Recognition of other countries’ trusted shipper programs.”.
SEC. 210. STRATEGIC PLAN TO ENHANCE THE SECURITY OF THE INTERNATIONAL SUPPLY CHAIN.

Paragraph (2) of section 201(g) of the Security and Accountability for Every Port Act of 2006 (6 U.S.C. 941) is amended to read as follows:

“(2) UPDATES.—Not later than 270 days after the date of the enactment of this paragraph and every three years thereafter, the Secretary shall submit to the appropriate congressional committees a report that contains an update of the strategic plan described in paragraph (1).”.

SEC. 211. CONTAINER SECURITY INITIATIVE.

Subsection (l) of section 205 of the Security and Accountability for Every Port Act of 2006 (6 U.S.C. 945) is amended—

(1) by striking “(1) IN GENERAL.—Not later than September 30, 2007,” and inserting “Not later than 270 days after the date of the enactment of the Border and Maritime Security Coordination Improvement Act,”;

(2) by redesignating subparagraphs (A) through (H) as paragraphs (1) through (8), respectively (and by moving the margins of such paragraphs 2 ems to the left); and

(3) by striking paragraph (2).
SEC. 212. TRANSPORTATION WORKER IDENTIFICATION CREDENTIAL WAIVER AND APPEALS PROCESS.

(a) In General.—Section 70105 of title 46, United States Code, is amended by adding at the end the following new section:

“(r) Securing the Transportation Worker Identification Credential Against Use by Unauthorized Aliens.—

“(1) In General.—The Secretary, acting through the Administrator of the Transportation Security Administration, shall seek to strengthen the integrity of transportation security cards issued under this section against improper access by an individual who is not lawfully present in the United States.

“(2) Components.—In carrying out subsection (a), the Administrator of the Transportation Security Administration shall—

“(A) publish a list of documents that will identify non-United States citizen transportation security card applicants and verify the immigration statuses of such applicants by requiring each such applicant to produce a document or documents that demonstrate—

“(i) identity; and
“(ii) proof of lawful presence in the United States; and

“(B) enhance training requirements to ensure that trusted agents at transportation security card enrollment centers receive training to identify fraudulent documents.

“(3) EXPIRATION.—A transportation security card issued under this section expires on the date of its expiration or on the date on which the individual to whom such card is issued is no longer lawfully entitled to be present in the United States, whichever is earlier.”.

(b) REPORT.—Not later than 90 days after the date of the enactment of this Act, the Secretary of Homeland Security shall provide to the Committee on Homeland Security of the House of Representatives and the Committee on Commerce, Science, and Transportation of the Senate information on the following:

(1) The average time for the completion of an appeal under the appeals process established pursuant to paragraph (4) of subsection (c) of section 70105 of title 46, United States Code.

(2) The most common reasons for any delays at each step in such process.
(3) Recommendations on how to resolve any such delays as expeditiously as possible.

SEC. 213. REPEALS.

The following provisions of the Security and Accountability for Every Port Act of 2006 (Public Law 109–347) are repealed:

(1) Section 105 (and the item relating to such section in the table of contents of such Act).

(2) Subsection (e) of section 108.

(3) Subsections (c), (d), and (e) of section 121 (6 U.S.C. 921).

(4) Section 122 (6 U.S.C. 922) (and the item relating to such section in the table of contents of such Act).

(5) Section 127 (and the item relating to such section in the table of contents of such Act).

(6) Subsection (c) of section 233 (6 U.S.C. 983).

(7) Section 235 (6 U.S.C. 984) (and the item relating to such section in the table of contents of such Act).

(8) Section 701 (and the item relating to such section in the table of contents of such Act).

(9) Section 708 (and the item relating to such section in the table of contents of such Act).
TITLE III—SECURING OUR
AGRICULTURE AND FOOD

SEC. 301. COORDINATION OF FOOD, AGRICULTURE, AND
VETERINARY DEFENSE AGAINST TERRORISM.

(a) In General.—Title V of the Homeland Security
Act of 2002 is amended by inserting after section 526 (6
U.S.C. 321o) the following new section:

“SEC. 527. COORDINATION OF DEPARTMENT OF HOMELAND
SECURITY EFFORTS RELATED TO FOOD, AG-
RICULTURE, AND VETERINARY DEFENSE
AGAINST TERRORISM.

“(a) Program Required.—The Secretary, acting
through the Assistant Secretary for Health Affairs, shall
carry out a program to coordinate the Department’s ef-
forts related to defending the food, agriculture, and veteri-
nary systems of the United States against terrorism and
other high-consequence events that pose a high risk to
homeland security.

“(b) Program Elements.—The coordination pro-
gram required by subsection (a) shall include, at a min-
imum, the following:

“(1) Providing oversight and management of
the Department’s responsibilities pursuant to Home-
land Security Presidential Directive 9—Defense of
United States Agriculture and Food.
“(2) Providing oversight and integration of the Department’s activities related to veterinary public health, food defense, and agricultural security.

“(3) Leading the Department’s policy initiatives relating to food, animal, and agricultural incidents, and the impact of such incidents on animal and public health.

“(4) Leading the Department’s policy initiatives relating to overall domestic preparedness for and collective response to agricultural terrorism.

“(5) Coordinating with other Department components, including U.S. Customs and Border Protection, as appropriate, on activities related to food and agriculture security and screening procedures for domestic and imported products.

“(6) Coordinating with appropriate Federal departments and agencies.

“(7) Other activities as determined necessary by the Secretary.”.

(b) CLERICAL AMENDMENT.—The table of contents in section 1(b) of the Homeland Security Act of 2002 (6 U.S.C. 101 note) is amended—

(1) by striking the items relating to sections 523, 524, and 525; and
(2) by inserting after the item relating to section 522 the following new items:

"Sec. 523. Guidance and recommendations.
Sec. 524. Voluntary private sector preparedness accreditation and certification program.
Sec. 525. Acceptance of gifts.
Sec. 526. Integrated public alert and warning system modernization.
Sec. 527. Coordination of Department of Homeland Security efforts related to food, agriculture, and veterinary defense against terrorism.".

TITLE IV—STRONG VISA INTEGRITY SECURES AMERICA

SEC. 401. VISA SECURITY.

(a) Visa Security Units at High Risk Posts.—

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

(1) by striking “The Secretary” and inserting the following:

“(A) AUTHORIZATION.—The Secretary”;

and

(2) by adding at the end the following new sub-

paragraph:

“(B) RISK-BASED ASSIGNMENTS.—

“(i) IN GENERAL.—The Secretary shall assign, in a risk-based manner, and based on the criteria described in clause (ii), employees of the Department to not fewer than 30 diplomatic and consular posts at which visas are issued.
“(ii) CRITERIA DESCRIBED.—The criteria referred to in clause (i) are the following:

“(I) The number of nationals of a country in which any of the diplomatic and consular posts referred to in clause (i) are located who were identified in United States Government databases related to the identities of known or suspected terrorists during the previous year.

“(II) The level of cooperation of such country with the counterterrorism efforts of the United States.

“(III) Information analyzing the presence, activity, or movement of terrorist organizations (as such term is defined in section 212(a)(3)(B)(vi) of the Immigration and Nationality Act (8 U.S.C. 1182(a)(3)(B)(vi))) within or through such country.

“(IV) The number of derogatory Security Advisory Opinions issued by the Visa Security Advisory Opinion Unit pursuant to paragraph (10) re-
garding nationals of a country in
which any of the diplomatic and con-
sular posts referred to in clause (i)
are located.

“(V) The adequacy of the border
and immigration control of such coun-
try.

“(VI) Any other criteria the Sec-
retary determines appropriate.

“(iii) RULE OF CONSTRUCTION.—The
assignment of employees of the Depart-
ment pursuant to this subparagraph is
solely the authority of the Secretary and
may not be altered or rejected by the Sec-
retary of State.”.

(b) COUNTERTERROR VETTING AND SCREENING.—
Paragraph (2) of section 428(e) of the Homeland Security
Act of 2002 is amended—

(1) by redesignating subparagraph (C) as sub-
paragraph (D); and

(2) by inserting after subparagraph (B) the fol-
lowing new subparagraph:

“(C) Screen any such applications against
the appropriate criminal, national security, and
terrorism databases maintained by the Federal Government.”.

(c) TRAINING AND HIRING.—Subparagraph (A) of section 428(e)(6) of the Homeland Security Act of 2002 is amended by—

(1) striking “The Secretary shall ensure, to the extent possible, that any employees” and inserting “The Secretary, acting through the Commissioner of U.S. Customs and Border Protection and the Director of U.S. Immigration and Customs Enforcement, shall provide training to any employees”; and

(2) striking “shall be provided the necessary training”.

(d) PRE-ADJUDICATED VISA SECURITY ASSISTANCE AND VISA SECURITY ADVISORY OPINION UNIT.—Subsection (e) of section 428 of the Homeland Security Act of 2002 is amended by adding at the end the following new paragraphs:

“(9) REMOTE PRE-ADJUDICATED VISA SECURITY ASSISTANCE.—At the visa-issuing posts at which employees of the Department are not assigned pursuant to paragraph (1), the Secretary shall, to the greatest extent possible, in a risk-based manner, and in consultation, where appropriate, with the Secretary of State, assign employees of the Department
to remotely perform the functions required under
paragraph (2) for such posts.

“(10) VISA SECURITY ADVISORY OPINION
UNIT.—The Secretary shall establish within U.S.
Immigration and Customs Enforcement a Visa Secu-
ritv Advisory Opinion Unit to respond to requests
from the Secretary of State to conduct a visa secu-
ritv review using information maintained by the De-
partment on visa applicants, including terrorism as-
sociation, criminal history, and other relevant fac-
tors, as determined by the Secretary.”.

SEC. 402. ELECTRONIC PASSPORT SCREENING AND BIO-
METRIC MATCHING.

(a) IN GENERAL.—Subtitle C of title IV of the
is amended by adding at the end the following new sec-
tions:

“SEC. 434. ELECTRONIC PASSPORT SCREENING AND BIO-
METRIC MATCHING.

“(a) IN GENERAL.—Not later than one year after the
date of the enactment of this section, the Commissioner
of U.S. Customs and Border Protection shall—

“(1) screen electronic passports at airports of
entry by reading each such passport’s embedded
chip; and
“(2) to the greatest extent practicable, utilize facial recognition technology or other biometric technology, as determined by the Commissioner, to screen travelers at United States airports of entry.

“(b) APPLICABILITY.—

“(1) ELECTRONIC PASSPORT SCREENING.—Paragraph (1) of subsection (a) shall apply to passports belonging to individuals who are United States citizens, individuals who are nationals of a program country pursuant to section 217 of the Immigration and Nationality Act (8 U.S.C. 1187), and individuals who are nationals of any other foreign country that issues electronic passports.

“(2) FACIAL RECOGNITION MATCHING.—Paragraph (2) of subsection (a) shall apply to individuals who are nationals of a program country pursuant to section 217 of the Immigration and Nationality Act.

“SEC. 435. CONTINUOUS SCREENING BY U.S. CUSTOMS AND BORDER PROTECTION.

“The Commissioner of U.S. Customs and Border Protection shall, in a risk based manner, continuously screen individuals issued any visa, and individuals who are nationals of a program country pursuant to section 217 of the Immigration and Nationality Act, who are present, or will soon be arriving, in the United States, against the
appropriate criminal, national security, and terrorism
databases maintained by the Federal Government.”.

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

"Sec. 434. Electronic passport screening and biometric matching.
"Sec. 435. Continuous screening by U.S. Customs and Border Protection.”.

SEC. 403. REPORTING OF VISA OVERSTAYS.

Section 2 of Public Law 105–173 (8 U.S.C. 1376)
is amended—

(1) in subsection (a)—

(A) by striking “Attorney General” and in-
serting “Secretary of Homeland Security”; and

(B) by inserting before the period at the
end the following: “, and any additional in-
formation that the Secretary determines necessary
for purposes of the report under subsection
(b)”; and

(2) by amending subsection (b) to read as fol-
lows:

“(b) ANNUAL REPORT.—Not later than June 30,
2017, and not later than June 30 of each year thereafter,
the Secretary of Homeland Security shall submit a report
to the Committee on Homeland Security and the Com-
mittee on the Judiciary of the House of Representatives
and to the Committee on Homeland Security and Governmental Affairs and the Committee on the Judiciary of the Senate providing, for the preceding fiscal year, numerical estimates of—

“(1) for each country, the number of aliens from the country who are described in subsection (a), including—

“(A) the total number of such aliens within all classes of nonimmigrant aliens described in section 101(a)(15) of the Immigration and Nationality Act (8 U.S.C. 1101(a)(15)); and

“(B) the number of such aliens within each of the classes of nonimmigrant aliens, as well as the number of such aliens within each of the subclasses of such classes of nonimmigrant aliens, as applicable;

“(2) for each country, the percentage of the total number of aliens from the country who were present in the United States and were admitted to the United States as nonimmigrants who are described in subsection (a);

“(3) the number of aliens described in subsection (a) who arrived by land at a port of entry into the United States; and
“(4) the number of aliens described in subsection (a) who entered the United States using a border crossing identification card (as such term is defined in section 101(a)(6) of the Immigration and Nationality Act (8 U.S.C. 1101(a)(6))).”.

SEC. 404. STUDENT AND EXCHANGE VISITOR INFORMATION SYSTEM VERIFICATION.

Not later than 90 days after the date of the enactment of this Act, the Secretary of Homeland Security shall ensure that the information collected under the program established under section 641 of the Illegal Immigration Reform and Immigrant Responsibility Act of 1996 (8 U.S.C. 1372) is available to officers of U.S. Customs and Border Protection conducting primary inspections of aliens seeking admission to the United States at each port of entry of the United States.
TITLE V—PROMOTING RESILIENCE AND EFFICIENCY IN PREPARING FOR ATTACKS AND RESPONDING TO EMERGENCIES

Subtitle A—Grants, Training, Exercises, and Coordination

SEC. 501. MEMORANDA OF UNDERSTANDING.

(a) IN GENERAL.—Subtitle B of title XX of the Homeland Security Act of 2002 (6 U.S.C. 611 et seq.) is amended by adding at the end the following new section:

“SEC. 2024. MEMORANDA OF UNDERSTANDING WITH DEPARTMENTAL COMPONENTS AND OFFICES.

“The Administrator shall enter into memoranda of understanding with the heads of the following departmental components and offices delineating the roles and responsibilities of such components and offices regarding the policy and guidance for grants under section 1406 of the Implementing Recommendations of the 9/11 Commission Act of 2007 (6 U.S.C. 1135), sections 2003 and 2004 of this Act, and section 70107 of title 46, United States Code, as appropriate:

“(1) The Commissioner of U.S. Customs and Border Protection.
“(2) The Administrator of the Transportation Security Administration.

“(3) The Commandant of the Coast Guard.

“(4) The Under Secretary for Intelligence and Analysis.

“(5) The Director of the Office of Emergency Communications.

“(6) The Assistant Secretary for State and Local Law Enforcement.

“(7) The Countering Violent Extremism Coordinator.

“(8) The Officer for Civil Rights and Civil Liberties.

“(9) The heads of other components or offices of the Department, as determined by the Secretary.”.

(b) CLERICAL AMENDMENT.—The table of contents in section 1(b) of the Homeland Security Act of 2002 is amended by inserting after the item relating to section 2023 the following new item:

“Sec. 2024. Memoranda of understanding with departmental components and offices.”.

SEC. 502. PERIOD OF PERFORMANCE.

(a) URBAN AREA SECURITY INITIATIVE.—Section 2003 of the Homeland Security Act of 2002 (6 U.S.C. 604) is amended by—
(1) redesignating subsection (e) as subsection (f); and

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

“(e) Period of Performance.—The Administrator shall make funds provided under this section available for use by a recipient of a grant for a period of not less than 36 months.”.

(b) State Homeland Security Grant Program.—Section 2004 of the Homeland Security Act of 2002 (6 U.S.C. 605) is amended by—

(1) redesignating subsection (f) as subsection (g); and

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

“(f) Period of Performance.—The Administrator shall make funds provided under this section available for use by a recipient of a grant for a period of not less than 36 months.”.

(c) Public Transportation Security Assistance Grant Program.—Section 1406 of the Implementing Recommendations of the 9/11 Commission Act (6 U.S.C. 1135; Public Law 110–53) is amended by—

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

•HR 6381 IH
(2) inserting after subsection (l) the following new subsection:

“(m) Period of Performance.—The Secretary shall make funds provided under this section available for use by a recipient of a grant for a period of not less than 36 months.”.

(d) Port Security Grant Program.—Section 70107 of title 46, United States Code, is amended by adding at the end the following new subsection:

“(n) Period of Performance.—The Secretary shall make funds provided under this section available for use by a recipient of a grant for a period of not less than 36 months.”.

(e) Tribal Security Grant Program.—Section 2005 of the Homeland Security Act of 2002 (6 U.S.C. 606) is amended by—

(1) redesignating subsections (h) through (k) subsections (i) through (l), respectively; and

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

“(h) Period of Performance.—The Secretary shall make funds provided under this section available for use by a recipient of a grant for a period of not less than 36 months.”.
SEC. 503. OPERATION STONEGARDEN.

(a) In General.—Subtitle A of title XX of the Homeland Security Act of 2002 (6 U.S.C. 601 et seq.) is amended by adding at the end the following new section:

"SEC. 2009. OPERATION STONEGARDEN.

"(a) Establishment.—There is established in the Department a program to be known as ‘Operation Stonegarden’. Under such program, the Secretary, acting through the Administrator, shall make grants to eligible law enforcement agencies, through the State Administrative Agency, to enhance border security in accordance with this section.

"(b) Eligible Recipients.—To be eligible to receive a grant under this section, a law enforcement agency shall—

"(1) be located in—

"(A) a State bordering either Canada or Mexico; or

"(B) a State or territory with a maritime border; and

"(2) be involved in an active, ongoing U.S. Customs and Border Protection operation coordinated through a sector office.

"(c) Permitted Uses.—The recipient of a grant under this section may use such grant for any of the following:

•HR 6381 IH
“(1) Equipment, including maintenance and sustainment costs.

“(2) Personnel, including overtime and backfill, in support of enhanced border law enforcement activities.


“(4) Any other appropriate activity, as determined by the Administrator, in consultation with the Commissioner of U.S. Customs and Border Protection.

“(d) Authorization of Appropriations.—There is authorized to be appropriated $55,000,000 for each of fiscal years 2016 through 2020 for grants under this section.

“(e) Report.—The Administrator shall annually for each of fiscal years 2016 through 2020 submit to the Committee on Homeland Security of the House of Representatives and the Committee on Homeland Security and Governmental Affairs of the Senate a report containing information on the expenditure of grants made under this section by each grant recipient.”.
(b) CONFORMING AMENDMENT.—Subsection (a) of section 2002 of the Homeland Security Act of 2002 (6 U.S.C. 603) is amended to read as follows:

“(a) GRANTS AUTHORIZED.—The Secretary, through the Administrator, may award grants under sections 2003, 2004, and 2009 to State, local, and tribal governments, as appropriate.”.

(c) CLERICAL AMENDMENT.—The table of contents in section 1(b) of the Homeland Security Act of 2002 is amended by inserting after the item relating to section 2008 the following new item:

“Sec. 2009. Operation Stonegarden.”.

SEC. 504. GRANTS METRICS.

(a) IN GENERAL.—To determine the extent to which grants under sections 2003 and 2004 of the Homeland Security Act of 2002 (6 U.S.C. 603 and 604) have closed capability gaps identified in State Preparedness Reports required under subsection (c) of section 652 of the Post-Katrina Emergency Management Reform Act of 2006 (6 U.S.C. 752; title VI of the Department of Homeland Security Appropriations Act, 2007; Public Law 109–295) and Threat and Hazard Identification and Risk Assessments from each State and high-risk urban area, the Administrator of the Federal Emergency Management Agency shall conduct and submit to the Committee on Homeland Security and the Committee on Transportation and Infra-

*HR 6381 IH*
structure of the House of Representatives and the Committee on Homeland Security and Governmental Affairs of the Senate an assessment of information provided in such Reports and Assessments.

(b) ASSESSMENT REQUIREMENTS.—The assessment required under subsection (a) shall include a comparison of successive State Preparedness Reports and Threat and Hazard Identification and Risk Assessments from each State and high-risk urban area.

SEC. 505. GRANT MANAGEMENT BEST PRACTICES.


SEC. 506. ADMINISTRATION AND COORDINATION OF GRANTS.

(a) IN GENERAL.—Paragraphs (1) and (2) of subsection (b) of section 2021 of the Homeland Security Act of 2002 (6 U.S.C. 611) are amended to read as follows:
“(1) IN GENERAL.—Any State or high-risk urban area receiving a grant under section 2003 or 2004 shall establish a State planning committee or urban area working group to assist in preparation and revision of the State, regional, or local homeland security plan or the threat and hazard identification and risk assessment, as the case may be, and to assist in determining effective funding priorities for grants under such sections 2003 and 2004.

“(2) COMPOSITION.—The State planning committees and urban area working groups referred to in paragraph (1) shall include at least one representative from each of the following significant stakeholders:

“(A) Local or tribal government officials.

“(B) Emergency response providers, including representatives of the fire service, law enforcement, emergency medical services, and emergency managers.

“(C) Public health officials and other appropriate medical practitioners.

“(D) Individuals representing educational institutions, including elementary schools, community colleges, and other institutions of higher education.
“(E) State and regional interoperable communications coordinators, as appropriate.

“(F) State and major urban area fusion centers, as appropriate.”.

(b) CONFORMING AMENDMENT.—Paragraph (3) of section 2021(b) (6 U.S.C. 611) is amended by inserting “or urban area working group, as the case may be,” after “planning committee”.

SEC. 507. FUNDING PROHIBITION.

The Secretary of Homeland Security may not implement the National Preparedness Grant Program or any successor grant program unless the Secretary receives prior authorization from Congress permitting such implementation.

SEC. 508. LAW ENFORCEMENT TERRORISM PREVENTION.

(a) LAW ENFORCEMENT TERRORISM PREVENTION PROGRAM.—Subsection (a) of section 2006 of the Homeland Security Act of 2002 (6 U.S.C. 607) is amended—

(1) in paragraph (1)—

(A) by inserting “States and high-risk urban areas use” after “that”; and

(B) by striking “is used”; and

(2) in paragraph (2), by amending subparagraph (I) to read as follows:
“(I) activities as determined appropriate by the Administrator, in coordination with the Assistant Secretary for State and Local Law Enforcement within the Office of Policy of the Department, through outreach to relevant stakeholder organizations.”.

(b) Office for State and Local Law Enforcement.—Subsection (b)(4) of section 2006 of the Homeland Security Act of 2002 (6 U.S.C. 607) is amended—

(1) in subparagraph (B), by inserting “, including through consultation with such agencies regarding Department programs that may impact such agencies” before the semicolon; and

(2) in subparagraph (D), by striking “ensure” and inserting “certify”.

SEC. 509. ALLOWABLE USES.

Subsection (a) of section 2008 of the Homeland Security Act of 2002 (6 U.S.C. 609) is amended—

(1) in the matter preceding paragraph (1), by inserting “including by working in conjunction with a National Laboratory (as defined in section 2(3) of the Energy Policy Act of 2005 (42 U.S.C. 15801(3))),” after “plans,”;

(2) by redesignating paragraphs (6) through (13) as paragraphs (7) through (14), respectively;
(3) by inserting after paragraph (5) the following new paragraph:

“(6) enhancing medical preparedness, medical surge capacity, and mass prophylaxis capabilities, including the development and maintenance of an initial pharmaceutical stockpile, including medical kits and diagnostics sufficient to protect first responders, their families, immediate victims, and vulnerable populations from a chemical or biological event;”;

and

(4) in subsection (b)(3)(B), by striking “(a)(10)” and inserting “(a)(11)”.

SEC. 510. MAINTENANCE OF GRANT INVESTMENTS.

Section 2008 of the Homeland Security Act of 2002 (6 U.S.C. 609) is amended by adding at the end the following new subsection:

“(g) MAINTENANCE OF EQUIPMENT.—Any applicant for a grant under section 2003 or 2004 seeking to use funds to purchase equipment, including pursuant to paragraph (3), (4), (5), or (9) of subsection (a) of this section, shall by the time of the receipt of such grant develop a plan for the maintenance of such equipment over its lifecycle that includes information identifying which entity is responsible for such maintenance.”.
SEC. 511. NATIONAL DOMESTIC PREPAREDNESS CONSORTIUM.

Section 1204 of the Implementing Recommendations of the 9/11 Commission Act (6 U.S.C. 1102) is amended—

(1) in subsection (d), by amending paragraphs (1) and (2) to read as follows:

“(1) for the Center for Domestic Preparedness, $65,000,000 for each of fiscal years 2016 and 2017; and

“(2) for the remaining Members of the National Domestic Preparedness Consortium, $98,000,000 for each of fiscal years 2016 and 2017.”; and

(2) in subsection (e), in the matter preceding paragraph (1), by striking “2007” and inserting “2015”.

SEC. 512. RURAL DOMESTIC PREPAREDNESS CONSORTIUM.

(a) IN GENERAL.—The Secretary of Homeland Security is authorized to establish a Rural Domestic Preparedness Consortium within the Department of Homeland Security consisting of universities and nonprofit organizations qualified to provide training to emergency response providers from rural communities.

(b) DUTIES.—The Rural Domestic Preparedness Consortium authorized under subsection (a) shall identify, develop, test, and deliver training to State, local, and trib-
al emergency response providers from rural communities, provide on-site and mobile training, and facilitate the de-
delivery of training by the training partners of the Depart-
ment of Homeland Security.

(c) Authorization of Appropriations.—Of amounts appropriated for Continuing Training Grants of the Department of Homeland Security, $5,000,000 is au-

thorized to be used for the Rural Domestic Preparedness Consortium authorized under subsection (a).

SEC. 513. EMERGENCY SUPPORT FUNCTIONS.

(a) Update.—Paragraph (13) of section 504(a) of the Homeland Security Act of 2002 (6 U.S.C. 314(a)) is amended by inserting “, periodically updating (but not less often than once every five years),” after “administering”.


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

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

“(d) Coordination.—The President, acting through the Administrator, shall develop and provide to Federal
departments and agencies with coordinating, primary, or
supporting responsibilities under the National Response
Framework performance metrics to ensure readiness to
execute responsibilities under the emergency support func-
tions of such Framework.”.

SEC. 514. REVIEW OF NATIONAL INCIDENT MANAGEMENT
SYSTEM.

Paragraph (2) of section 509(b) of the Homeland Se-
curity Act of 2002 (6 U.S.C. 319(b)) is amended, in the
matter preceding subparagraph (A), by inserting “, but
not less often than once every five years,” after “periodi-
cally”.

SEC. 515. APPROVAL OF CERTAIN EQUIPMENT.

Section 2008 of the Homeland Security Act of 2002
(6 U.S.C. 609) is amended by adding at the end the fol-
lowing:

“(g) REVIEW PROCESS.—The Administrator shall de-
velop and implement a uniform process for reviewing ap-
plications to use grants provided under section 2003 or
2004 to purchase equipment or systems not included on
the Authorized Equipment List maintained by the Admin-
istrator.”.

SEC. 516. REMEDIAL ACTION MANAGEMENT PROGRAM.

Section 650 of the Post-Katrina Emergency Manage-
ment Reform Act of 2006 (6 U.S.C. 750; title VI of the
Department of Homeland Security Appropriations Act, 2007; Public Law 109–295) is amended to read as follows:

“SEC. 650. REMEDIAL ACTION MANAGEMENT PROGRAM.

“(a) In General.—The Administrator, in coordination with the National Council on Disability and the National Advisory Council, shall establish a remedial action management program to—

“(1) analyze training, exercises, and real world events to identify lessons learned, corrective actions, and best practices;

“(2) generate and disseminate, as appropriate, the lessons learned, corrective actions, and best practices referred to in paragraph (1); and

“(3) conduct remedial action tracking and long term trend analysis.

“(b) Federal Corrective Actions.—The Administrator, in coordination with the heads of appropriate Federal departments and agencies, shall utilize the program established in subsection (a) to collect information on corrective actions identified by such Federal departments and agencies during exercises and the response to natural disasters, acts of terrorism, and other man-made disasters, and shall, not later than one year after the date of the enactment of this section and annually thereafter
for each of the next four years, submit to Congress a re-
port on the status of such corrective actions.

“(c) DISSEMINATION OF AFTER ACTION REPORTS.—
The Administrator shall provide electronically, to the max-
imum extent practicable, to Congress and Federal, State,
local, tribal, and private sector officials after-action re-
ports and information on lessons learned and best prac-
tices from responses to acts of terrorism, natural disas-
ters, capstone exercises conducted under the national exer-
cise program under section 648(b), and other emergencies
or exercises.”.

Subtitle B—Communications

SEC. 521. OFFICE OF EMERGENCY COMMUNICATIONS.
The Secretary of Homeland Security may not change
the location or reporting structure of the Office of Emer-
gency Communications of the Department of Homeland
Security unless the Secretary receives prior authorization
from the Committee on Homeland Security of the House
of Representatives and the Committee on Homeland Secu-
rity and Governmental Affairs of the Senate permitting
such change.

SEC. 522. RESPONSIBILITIES OF OFFICE OF EMERGENCY

COMMUNICATIONS DIRECTOR.

Subsection (c) of section 1801 of the Homeland Secu-

rity Act of 2002 (6 U.S.C. 571) is amended—
(1) by striking paragraph (3);

(2) by redesignating paragraphs (4) through (15) as paragraphs (3) through (14), respectively;

(3) in paragraph (8), as so redesignated, by striking “, in cooperation with the National Communications System,”;

(4) in paragraph (9), as so redesignated, by striking “the Homeland Security Council,”;

(5) in paragraph (12) by striking “Assistant Secretary for Grants and Training” and inserting “Assistant Administrator of the Grant Programs Directorate of the Federal Emergency Management Agency”;

(6) in paragraph (13), as so redesignated, by striking “and” at the end; and

(7) by adding after paragraph (14), as so redesignated, the following new paragraphs:

“(15) administer the Government Emergency Telecommunications Service (GETS) and Wireless Priority Service (WPS) programs, or successor programs; and

“(16) assess the impact of emerging technologies on interoperable emergency communications.”.
SEC. 523. ANNUAL REPORTING ON ACTIVITIES OF THE OFFICE OF EMERGENCY COMMUNICATIONS.

Subsection (f) of section 1801 of the Homeland Security Act of 2002 (6 U.S.C. 571) is amended to read as follows:

“(f) ANNUAL REPORTING OF OFFICE ACTIVITIES.—

The Director of the Office of Emergency Communications shall, not later than one year after the date of the enactment of this subsection and annually thereafter for each of the next four years, report to the Committee on Homeland Security and the Committee on Energy and Commerce of the House of Representatives and the Committee on Homeland Security and Governmental Affairs of the Senate on the activities and programs of the Office, including specific information on efforts to carry out paragraphs (4), (5), and (6) of subsection (c).”.

SEC. 524. NATIONAL EMERGENCY COMMUNICATIONS PLAN.

Section 1802 of the Homeland Security Act of 2002 (6 U.S.C. 572) is amended—

(1) in subsection (a), in the matter preceding paragraph (1)—

(A) by striking “, and in cooperation with the Department of National Communications System (as appropriate),”; and

(B) by inserting “, but not less than once every five years,” after “periodically”; and
(2) in subsection (c)—

(A) by redesignating paragraphs (3) through (10) as paragraphs (4) through (11), respectively; and

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

“(3) consider the impact of emerging technologies on the attainment of interoperable emergency communications;”.

SEC. 525. TECHNICAL EDITS.

Title XVIII of the Homeland Security Act of 2002 is amended—

(1) in subsection (d) of section 1801 (6 U.S.C. 571) by—

(A) striking paragraph (2); and

(B) redesignating paragraph (3) as paragraph (2); and

(2) in paragraph (1) of section 1804(b) (6 U.S.C. 574(b)), in the matter preceding subparagraph (A), by striking “Assistant Secretary for Grants and Planning” and inserting “Assistant Administrator of the Grant Programs Directorate of the Federal Emergency Management Agency”.

•HR 6381 IH
SEC. 526. PUBLIC SAFETY BROADBAND NETWORK.

The Undersecretary of the National Protection and Programs Directorate of the Department of Homeland Security shall submit to the Committee on Homeland Security and the Committee on Energy and Commerce of the House of Representatives and the Committee on Homeland Security and Governmental Affairs of the Senate information on the Department of Homeland Security’s responsibilities related to the development of the nationwide Public Safety Broadband Network authorized in section 6202 of the Middle Class Tax Relief and Job Creation Act of 2012 (47 U.S.C. 1422; Public Law 112–96), including information on efforts by the Department to work with the First Responder Network Authority of the Department of Commerce to identify and address cyber risks that could impact the near term or long term availability and operations of such network and recommendations to mitigate such risks.

SEC. 527. STATEWIDE INTEROPERABILITY COORDINATORS.

(a) In general.—Paragraph (2) of section 2004(b) of the Homeland Security Act of 2002 (6 U.S.C. 605(b)) is amended by—

(1) redesignating subparagraphs (B) and (C) as subparagraphs (C) and (D), respectively; and

(2) inserting after subparagraph (A) the following new subparagraph:
“(B)(i) certification that the Governor of
the State has designated a Statewide Interoper-
ability Coordinator, including identification in
such certification of the individual so des-
ignated, who shall be responsible for—

“(I) coordinating the daily operations
of the State’s interoperability efforts;

“(II) coordinating State interoper-
ability and communications projects and
grant applications for such projects;

“(III) establishing and maintaining
working groups to develop and implement
key interoperability initiatives; and

“(IV) coordinating and updating, as
necessary, a Statewide Communications
Interoperability Plan that specifies the cur-
rent status of State efforts to enhance
communications interoperability within the
State, including progress, modifications, or
setbacks, and future goals for communica-
tions interoperability among emergency re-
ponse agencies in the State; or

“(ii) if a Statewide Interoperability Coordi-
nator has not been designated in accordance
with clause (i)—
“(I) certification that the State is performing in another manner the functions described in subclauses (I) through (IV) of such clause; and

“(II) identification in such certification of an individual who has been designated by the State as the primary point of contact for performance of such functions;”.

(b) LIMITATION ON APPLICATION.—The amendment made by subsection (a) shall not apply with respect to any grant for which an application was submitted under the State Homeland Security Grant Program under section 2004 of the Homeland Security Act of 2002 (6 U.S.C. 605) before the date of the enactment of this section.

SEC. 528. COMMUNICATIONS TRAINING.

The Under Secretary for Management of the Department of Homeland Security, in coordination with the appropriate component heads, shall develop a mechanism, consistent with the strategy required pursuant to the Department of Homeland Security Interoperable Communications Act (Public Law 114–29), to verify that radio users within the Department receive initial and ongoing training on the use of the radio systems of such components, including interagency radio use protocols.
Subtitle C—Medical Preparedness

SEC. 531. PRE-EVENT ANTHRAX VACCINATION PROGRAM FOR EMERGENCY RESPONSE PROVIDERS.

(a) Anthrax Preparedness.—

(1) In general.—Title V of the Homeland Security Act of 2002 (6 U.S.C. 311 et seq.) is amended by adding at the end the following new section:

“SEC. 526. ANTHRAX PREPAREDNESS.

“(a) Pre-Event Anthrax Vaccination Program for Emergency Response Providers.—For the purpose of domestic preparedness for and collective response to terrorism, the Secretary, in coordination with the Secretary of Health and Human Services, shall establish a program to provide anthrax vaccines from the strategic national stockpile under section 319F–2(a) of the Public Health Service Act (42 U.S.C. 247d–6b(a)) that will be nearing the end of their labeled dates of use at the time such vaccines are to be administered to emergency response providers who are at high risk of exposure to anthrax and who voluntarily consent to such administration, and shall—

“(1) establish any necessary logistical and tracking systems to facilitate making such vaccines so available;
“(2) distribute disclosures regarding associated benefits and risks to end users; and

“(3) conduct outreach to educate emergency response providers about the voluntary program.

“(b) THREAT ASSESSMENT.—The Secretary shall—

“(1) support homeland security-focused risk analysis and risk assessments of the threats posed by anthrax from an act of terror;

“(2) leverage existing and emerging homeland security intelligence capabilities and structures to enhance prevention, protection, response, and recovery efforts with respect to an anthrax terror attack; and

“(3) share information and provide tailored analytical support on threats posed by anthrax to State, local, and tribal authorities, as well as other national biosecurity and biodefense stakeholders.”

(2) CLERICAL AMENDMENT.—The table of contents in section 1(b) of the Homeland Security Act of 2002 is amended by inserting at the end of the items relating to title V the following new item:

“Sec. 526. Anthrax preparedness.”.

(b) PILOT PROGRAM.—

(1) IN GENERAL.—In carrying out the pre-event vaccination program authorized in subsection (a) of section 526 of the Homeland Security Act of

HR 6381 IH
2002, as added by subsection (a) of this section, the Secretary of Homeland Security, in coordination with the Secretary of Health and Human Services, shall carry out a pilot program to provide anthrax vaccines to emergency response providers as so authorized. The duration of the pilot program shall be 24 months from the date the initial vaccines are administered to participants.

(2) Preliminary requirements.—Prior to implementing the pilot program under paragraph (1), the Secretary of Homeland Security shall—

(A) establish a communication platform for such pilot program;

(B) establish education and training modules for such pilot program;

(C) conduct economic analysis of such pilot program; and

(D) create a logistical platform for the anthrax vaccine request process under such pilot program.

(3) Location.—In carrying out the pilot program under paragraph (1), the Secretary of Homeland Security shall select emergency response providers based in at least two States for participation in such pilot program.
(4) **Distribution of Information.**—The Secretary of Homeland Security shall provide to each emergency response provider who participates in the pilot program under paragraph (1) disclosures and educational materials regarding the associated benefits and risks of any vaccine provided under such pilot program and of exposure to anthrax.

(5) **Report.**—Not later than one year after the date of the enactment of this Act and annually thereafter until one year after the completion of the pilot program under paragraph (1), the Secretary of Homeland Security shall submit to the Committee on Homeland Security and the Committee on Energy and Commerce of the House of Representatives and the Committee on Homeland Security and Governmental Affairs of the Senate a report on the progress and results of such pilot program, including the percentage of eligible emergency response providers, as determined by each pilot location, that volunteer to participate, the degree to which participants obtain necessary vaccinations, as appropriate, and recommendations to improve initial and recurrent participation in such pilot program. Each such report shall include a discussion of plans to continue such pilot program to provide vaccines to emergency
response providers under subsection (a) of section 526 of the Homeland Security Act of 2002, as added by subsection (a) of this section.

(6) DEADLINE FOR IMPLEMENTATION.—The Secretary of Homeland Security shall begin implementing the pilot program under paragraph (1) by not later than the date that is one year after the date of the enactment of this Act.

SEC. 532. CHIEF MEDICAL OFFICER.

(a) IN GENERAL.—Subsection (c) of section 516 of the Homeland Security Act of 2002 (6 U.S.C. 321e) is amended—

(1) in the matter preceding paragraph (1), by inserting “and shall establish medical and human, animal, and occupational health exposure policy, guidance, strategies, and initiatives,” before “including—”;

(2) in paragraph (1), by inserting before the semicolon at the end the following: “, including advice on how to prepare for, protect against, respond to, recover from, and mitigate against the medical effects of terrorist attacks or other high consequence events utilizing chemical, biological, radiological, or nuclear agents or explosives”;
(3) in paragraph (2), by inserting before the semicolon at the end the following: “, including co-
ordinating the Department’s policy, strategy and preparedness for pandemics and emerging infectious diseases”;

(4) in paragraph (5), by inserting “emergency medical services and medical first responder stake-
holders,” after “the medical community”;

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

(6) by adding after paragraph (7) the following new paragraphs:

“(8) ensuring that the workforce of the Depart-
ment has evidence-based policy, standards, require-
ments, and metrics for occupational health and opera-
tional medicine programs;

“(9) directing and maintaining a coordinated system for medical support for the Department’s operational activities;

“(10) providing oversight of the Department’s medical programs and providers, including—

“(A) reviewing and maintaining verification of the accreditation of the Depart-
ment’s health provider workforce;
“(B) developing quality assurance and clinical policy, requirements, standards, and metrics for all medical and health activities of the Department;

“(C) providing oversight of medical records systems for employees and individuals in the Department’s care and custody; and

“(D) providing medical direction for emergency medical services activities of the Department; and

“(11) as established under section 527, maintaining a medical countermeasures stockpile and dispensing system, as necessary, to facilitate personnel readiness, and protection for working animals, employees, and individuals in the Department’s care and custody in the event of a chemical, biological, radiological, nuclear, or explosives attack, naturally occurring disease outbreak, or pandemic.”.

(b) MEDICAL LIAISONS.—The Chief Medical Officer of the Department of Homeland Security may provide medical liaisons to the components of the Department to provide subject matter expertise on medical and public health issues and a direct link to the Chief Medical Officer. Such expertise may include the following:
(1) Providing guidance on health and medical aspects of policy, planning, operations, and workforce health protection.

(2) Identifying and resolving component medical issues.

(3) Supporting the development and alignment of medical and health systems.

(4) Identifying common gaps in medical and health standards, policy, and guidance, and enterprise solutions to bridge such gaps.

SEC. 533. MEDICAL COUNTERMEASURES PROGRAM.

(a) In General.—Title V of the Homeland Security Act of 2002 (6 U.S.C. 311 et seq.), as amended by section 531 of this title, is further amended by adding at the end the following new section:

“SEC. 527. MEDICAL COUNTERMEASURES.

“(a) In General.—The Secretary shall establish a medical countermeasures program to facilitate personnel readiness, and protection for working animals, employees, and individuals in the Department’s care and custody, in the event of a chemical, biological, radiological, nuclear, or explosives attack, naturally occurring disease outbreak, or pandemic, and to support Department mission continuity.”
“(b) OVERSIGHT.—The Chief Medical Officer, established under section 516, shall provide programmatic oversight of the medical countermeasures program established pursuant to subsection (a), and shall—

“(1) develop Department-wide standards for medical countermeasure storage, security, dispensing, and documentation;

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

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

“(4) provide oversight and guidance on dispensing of stockpiled medical countermeasures;

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

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

“(7) support dispensing exercises.

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

“(d) MEDICAL COUNTERMEASURES MANAGEMENT.—Not later than 180 days after the date of the enactment of this section, the Chief Medical Officer shall develop and submit to the Secretary an integrated logistics support plan for medical countermeasures, including—

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

“(2) a replenishment plan; and

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

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

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

“(2) Centers for Disease Control and Prevention guidance on medical countermeasures.
“(f) REPORT.—No later than 180 days after the date of the enactment of this section, the Chief Medical Officer shall report to the Committee on Homeland Security of the House of Representatives and the Committee on Homeland Security and Governmental Affairs of the Senate on progress in achieving the requirements of this section.”.

(b) CLERICAL AMENDMENT.—The table of contents in section 1(b) of the Homeland Security Act of 2002, as amended by section 531 of this title, is further amended by inserting at the end of the items relating to title V the following new item:

“Sec. 527. Medical countermeasures.”.

Subtitle D—Management

SEC. 541. MISSION SUPPORT.

(a) ESTABLISHMENT.—The Administrator of the Federal Emergency Management Agency shall designate an individual to serve as the chief management official and principal advisor to the Administrator on matters related to the management of the Federal Emergency Management Agency, including management integration in support of emergency management operations and programs.

(b) MISSION AND RESPONSIBILITIES.—The Administrator of the Federal Emergency Management Agency, acting through the official designated pursuant to subsection (a), shall be responsible for the management and
administration of the Federal Emergency Management
Agency, including with respect to the following:

(1) Procurement.

(2) Human resources and personnel.

(3) Information technology and communications systems.

(4) Real property investment and planning, facilities, accountable personal property (including fleet and other material resources), records and disclosure, privacy, safety and health, and sustainability and environmental management.

(5) Security for personnel, information technology and communications systems, facilities, property, equipment, and other material resources.

(6) Any other management duties that the Administrator may designate.

(c) MOUNT WEATHER EMERGENCY OPERATIONS AND ASSOCIATED FACILITIES.—Nothing in this section shall be construed as limiting or otherwise affecting the role or responsibility of the Assistant Administrator for National Continuity with respect to the matters described in subsection (b) as they relate to the Mount Weather Emergency Operations Center and associated facilities. The management and administration of the Mount Weather Emergency Operations Center and associated facilities
remains the responsibility of the Assistant Administrator for National Continuity.

(d) REPORT.—Not later than 270 days after the date of the enactment of this Act, the Administrator of the Federal Emergency Management Agency shall submit to the Committee on Homeland Security and the Committee on Transportation and Infrastructure of the House of Representatives and the Committee on Homeland Security and Governmental Affairs of the Senate a report that includes—

(1) a review of financial, human capital, information technology, real property planning, and acquisition management of headquarters and all regional offices of the Federal Emergency Management Agency; and

(2) a strategy for capturing financial, human capital, information technology, real property planning, and acquisition data.

SEC. 542. SYSTEMS MODERNIZATION.

Not later than 120 days after the date of the enactment of this Act, the Administrator of the Federal Emergency Management Agency shall submit to the Committee on Homeland Security and the Committee on Transportation and Infrastructure of the House of Representatives and the Committee on Homeland Security and Government-
mental Affairs of the Senate a report on the Federal Emergency Management Agency’s efforts to modernize its grants and financial information technology systems, including the following:

1. A summary of all previous efforts to modernize such systems.
2. An assessment of long term cost savings and efficiencies gained through such modernization effort.
3. A capability needs assessment.
4. Estimated quarterly costs.
5. Estimated acquisition life cycle dates, including acquisition decision events.

SEC. 543. STRATEGIC HUMAN CAPITAL PLAN.

Subsection (c) of section 10102 of title 5, United States Code, is amended by striking “2007” and inserting “2016”.

SEC. 544. ACTIVITIES RELATED TO CHILDREN.

Paragraph (2) of section 503(b) of the Homeland Security Act of 2002 (6 U.S.C. 313(b)) is amended—

1. in subparagraph (G), by striking “and” at the end;
2. in subparagraph (H), by striking the period at the end and inserting “; and”; and
(3) by adding at the end the following new sub-
paragraph:

“(I) integrate the needs of children into
the Agency’s activities to prepare for, protect
against, respond to, recover from, and mitigate
against natural disasters, acts of terrorism, and
other man-made disasters, including by appoint-
ing a technical expert to coordinate such activi-
ties, as necessary.”.

Subtitle E—Flood Insurance
Claims Process Reforms

SEC. 551. CLAIMS ADJUSTMENT AND ENGINEERING RE-
PORTS.

Section 1312 of the National Flood Insurance Act of
1968 (42 U.S.C. 4019) is amended by adding at the end
the following new subsections:

“(d) FINAL ENGINEERING REPORTS.—The Adminis-
trator shall require that, in the case of any on-site inspec-
tion of a property by an engineer for the purpose of assess-
ing any claim for losses covered by a policy for flood insur-
ance coverage provided under this title, the final engineer-
ing report shall be provided to the insured under the pol-
icy, as follows:

“(1) TIMING.—The final engineering report
may not be transmitted to any other person, em-
ployer, agency, or entity, before it is transmitted to
the insured.

“(2) Prohibition on alterations; certification.—The final engineering report may not in-
clude alterations by, or at the request of, anyone
other than the responsible in charge for such report
and shall include a certification, signed by the re-
sponsible in charge for the report, that it does not
contain any such alterations.

“(3) Transmittal.—The final engineering re-
port shall be transmitted to the insured in a manner
as the Administrator shall provide that provides rea-
sonable assurance that it was transmitted directly to
the insured by the responsible in charge.

“(4) Reports covered.—For purposes of this
subsection, the term ‘final engineering report’ means
an engineering report, survey, or other document in
connection with such claim that—

“(A) is based on such on-site inspection;

“(B) contains final conclusions with re-
spect to an engineering issue or issues involved
in such claim; and

“(C) is signed by the responsible in charge
or affixed with the seal of such responsible in
charge, or both.
“(e) CLAims ADJUSTMENT REPORTS.—The Administrator shall require that, in the case of any on-site inspection of a property by a claims adjustor for the purpose of assessing any claim for losses covered by a policy for flood insurance coverage provided under this title, any report shall be provided to the insured under the policy, as follows:

“(1) TIMING.—Such report may not be transmitted to any other person, employer, agency, or entity, before it is transmitted to the insured.

“(2) PROHIBITION ON ALTERATIONS; CERTIFICATION.—The report may not include alterations by, or at the request of, anyone other than such preparer and shall include a certification, signed by the preparer of the report, that it does not contain any such alterations.

“(3) TRANSMITTAL.—The report shall be transmitted to the insured in a manner as the Administrator shall provide that provides reasonable assurance that it was transmitted directly to the insured by the preparer.

“(4) REPORTS COVERED.—For purposes of this subsection, the term ‘report’ means any report or document in connection with such claim that is based on such on-site inspection by the claims adjus-
tor, including any adjustment report and field report. Such term also includes any draft, preliminary version, or copy of any such report and any amendments or additions to any such report. Such term does not include any engineering report, as such term is defined for purposes of subsection (d).”.

SEC. 552. JUDICIAL REVIEW.

(a) GOVERNMENT PROGRAM WITH INDUSTRY ASSISTANCE.—Section 1341 of the National Flood Insurance Act of 1968 (42 U.S.C. 4072) is amended by striking “within one year after the date of mailing of notice of disallowance or partial disallowance by the Administrator” and inserting the following: “not later than the expiration of the 2-year period beginning upon the date of the occurrence of the losses involved in such claim or, in the case of a denial of a claim for losses that is appealed to the Administrator, not later than (1) the expiration of the 90-day period beginning upon the date of a final determination upon appeal denying such claim in whole or in part, or (2) the expiration of such 2-year period, whichever is later”.

(b) INDUSTRY PROGRAM WITH FEDERAL FINANCIAL ASSISTANCE.—Section 1333 of the National Flood Insurance Act of 1968 (42 U.S.C. 4053) is amended by striking “within one year after the date of mailing of notice of dis-
allowance or partial disallowance of the claim” and inserting the following: “not later than the expiration of the 2-year period beginning upon the date of the occurrence of the losses involved in such claim or, in the case of a denial of a claim for losses that is appealed to the Administrator, not later than (1) the expiration of the 90-day period beginning upon the date of a final determination upon appeal denying such claim in whole or in part, or (2) the expiration of such 2-year period, whichever is later”.

**TITLE VI—CYBERSECURITY AND INFRASTRUCTURE PROTECTION AGENCY**

**SEC. 601. CYBERSECURITY AND INFRASTRUCTURE PROTECTION AGENCY.**

(a) IN GENERAL.—The Homeland Security Act of 2002 is amended by adding at the end the following new title:

“**TITLE XXII—CYBERSECURITY AND INFRASTRUCTURE PROTECTION AGENCY**

“Subtitle A—Cybersecurity and Infrastructure Protection

“SEC. 2201. DEFINITIONS.

“In this subtitle—
“(1) Critical infrastructure incident.—The term ‘critical infrastructure incident’ means an occurrence that actually or immediately jeopardizes, without lawful authority, the integrity, confidentiality, or availability of critical infrastructure.

“(2) Critical infrastructure information.—The term ‘critical infrastructure information’ has the meaning given such term in section 2215.

“(3) Critical infrastructure risk.—The term ‘critical infrastructure risk’ means threats to and vulnerabilities of critical infrastructure and any related consequences caused by or resulting from unauthorized access, use, disclosure, degradation, disruption, modification, or destruction of such critical infrastructure, including such related consequences caused by an act of terrorism.

“(4) Cybersecurity risk.—The term ‘cybersecurity risk’ has the meaning given such term in section 2209.

“(5) Cybersecurity threat.—The term ‘cybersecurity threat’ has the meaning given such term in paragraph (5) of section 102 of the Cybersecurity Information Sharing Act of 2015 (contained in division N of the Consolidated Appropriations Act, 2016 (Public Law 114–113; 6 U.S.C. 1501)).
“(6) FEDERAL ENTITY.—The term ‘Federal entity’ has the meaning given such term in paragraph (8) of section 102 of the Cybersecurity Information Sharing Act of 2015 (contained in division N of the Consolidated Appropriations Act, 2016 (Public Law 114–113; 6 U.S.C. 1501)).

“(7) NON-FEDERAL ENTITY.—The term ‘non-Federal entity’ has the meaning given such term in paragraph (14) of section 102 of the Cybersecurity Information Sharing Act of 2015 (contained in division N of the Consolidated Appropriations Act, 2016 (Public Law 114–113; 6 U.S.C. 1501)).

“(8) SHARING.—The term ‘sharing’ has the meaning given such term in section 2209.

“SEC. 2202. CYBERSECURITY AND INFRASTRUCTURE PROTECTION AGENCY.

“(a) REDESIGNATION.—

“(1) IN GENERAL.—The National Protection and Programs Directorate of the Department shall, on and after the date of the enactment of this subtitle, be known as the ‘Cybersecurity and Infrastructure Protection Agency’ (in this subtitle referred to as the ‘Agency’).

“(2) REFERENCES.—Any reference to the National Protection and Programs Directorate of the
Department in any law, regulation, map, document, record, or other paper of the United States shall be deemed to be a reference to the Cybersecurity and Infrastructure Protection Agency of the Department.

“(b) MISSION.—The mission of the Agency shall be to lead national efforts to protect and enhance the security and resilience of the cyber and critical infrastructure of the United States.

“(c) DIRECTOR.—

“(1) IN GENERAL.—The Agency shall be headed by a Director of National Cybersecurity (in this subtitle referred to as the ‘Director’).

“(2) REFERENCE.—Any reference to an Under Secretary responsible for overseeing critical infrastructure protection, cybersecurity, and any other related program of the Department as described in section 103(a)(1)(H) as in effect on the day before the date of the enactment of this subtitle in any law, regulation, map, document, record, or other paper of the United States shall be deemed to be a reference to the Director of National Cybersecurity of the Department.

“(d) RESPONSIBILITIES.—The Director shall—
“(1) lead cybersecurity and critical infrastructure protection policy and operations for the Department;

“(2) serve as the primary representative of the Department for coordinating with Federal entities, non-Federal entities, and international partners the cybersecurity and critical infrastructure protection policy and operations referred to in paragraph (1);

“(3) facilitate a national effort to strengthen and maintain secure, functioning, and resilient critical infrastructure from threats;

“(4) maintain and utilize mechanisms, including a coordinating body for the regular and ongoing consultation and collaboration among the Agency’s Divisions to further operation coordination, integrated situational awareness, and improved integration across the Agency;

“(5) develop, coordinate, and implement—

“(A) comprehensive strategic plans for cybersecurity and critical infrastructure protection; and

“(B) risk assessments for the Department, in accordance with subsection (f);

“(6) carry out emergency communications responsibilities, in accordance with title XVIII;
“(7) carry out the authorities designated to the Secretary under section 1315 of title 40 United States Code; and

“(8) carry out such other duties and powers prescribed by law or delegated by the Secretary.

“(e) RISK ASSESSMENTS.—

“(1) NATIONAL RISK ASSESSMENTS.—The Director, in coordination with the heads of relevant components of the Department and other appropriate Federal entities, shall develop, coordinate, and update periodically (not less often than once every two years) a national risk assessment of—

“(A) cybersecurity risks; and

“(B) critical infrastructure risks.

“(2) INTEGRATED NATIONAL RISK ASSESSMENTS.—The Director shall develop, coordinate, and update periodically (not less often than once every two years) an integrated national risk assessment that assesses all of the cybersecurity risks and critical infrastructure risks referred to in paragraph (1) and compares each such risk and incident against one another according to their relative risk, including cascading effects between each such risk.

“(3) INCLUSION IN ASSESSMENTS.—Each national risk assessment required under paragraph (1)
and integrated national risk assessment required under paragraph (2) shall include—

“(A) a description of the data and methodology used for each such assessment; and

“(B) if applicable, actions or countermeasures recommended or taken by the Secretary or the head of another Federal agency to address issues identified in each such assessment.

“(4) CLASSIFICATION.—The Director shall ensure that each national risk assessment required under paragraph (1) and integrated national risk assessment required under paragraph (2) has a classified and unclassified version.

“(5) PROVISION TO CONGRESS.—The Director shall provide to the Committee on Homeland Security of the House of Representatives and the Committee on Homeland Security and Governmental Affairs of the Senate each national risk assessment required under paragraph (1) and integrated national risk assessment required under paragraph (2) not later than 30 days after the completion of each such assessment.

“(f) METHODOLOGY.—In developing each national risk assessment required under subsection (f)(1) and inte-
grated national risk assessment required under subsection (g)(2), the Director, in consultation with the heads of relevant Federal entities, shall—

“(1) assess the proposed methodology to be used for such assessments; and

“(2) consider the evolving threat to the United States as indicated by the intelligence community (as such term is defined in section 3(4) of the National Security Act of 1947 (50 U.S.C. 3003(4))). “

“(g) USAGE.—The national risk assessments and integrated national risk assessments required under subsection (f) shall be used to inform and guide allocation of resources for cybersecurity and critical infrastructure protection activities of the Department.

“(h) INPUT AND SHARING.—The Director shall, for each national risk assessment and integrated national risk assessment required under subsection (f)—

“(1) seek input from relevant Federal and non-Federal entities involved in efforts to counter threats;

“(2) ensure that written procedures are in place to guide the development of such assessments, including for input, review, and implementation purposes, among relevant Federal entities;
“(3) share the classified versions of such assessments with appropriate representatives from relevant Federal and non-Federal entities with appropriate security clearances and a need for such assessments; and

“(4) to the maximum extent practicable, make available the unclassified versions of such assessments to relevant Federal and non-Federal entities for cybersecurity and critical infrastructure protection.

“(i) COMPOSITION.—The Agency shall be composed of the following divisions:

“(1) The Cybersecurity Division, headed by a Principal Deputy Director.

“(2) The Infrastructure Protection Division, headed by a Deputy Director.

“(3) The Emergency Communications Division under title XVIII, headed by a Deputy Director.

“(4) The Federal Protective Service, headed by a Deputy Director.

“(j) CONTRACTING AUTHORITY.—

“(1) DEFINITION.—In this subsection the term ‘head of contracting activity’ means each official responsible for the creation, management, and oversight of a team of procurement professionals prop-
erly trained, certified, and warranted to accomplish
the acquisition of products and services on behalf of
the designated components, offices, and organiza-
tions of the Department, and as authorized, other
Federal Government entities.

“(2) APPLICATION.—All procurement and con-
tracting activities for the Agency shall be performed
in accordance with the Federal Acquisition Regula-
tion, the Department of Homeland Security Acquisi-
tion Policy, and other applicable laws, Federal regu-
lations, and policies.

“(3) DELEGATED AUTHORITY.—The Secretary,
acting through the Chief Procurement Officer of the
Department, may delegate procurement and con-
tracting authority to the Agency head of contracting
activity, as appropriate, after—

“(A) verifying that the head of contracting
activity has the training and experience to carry
out the authority to be delegated;

“(B) validating that Agency has identified
the personnel, systems, and resources to carry
out the authority to be delegated; and

“(C) providing Congress with a notification
of the delegation and attestations under para-
graphs (1) and (2).
“(4) PERFORMANCE REVIEW.—

“(A) IN GENERAL.—The Chief Procurement Officer shall provide input on the periodic performance review of the Agency’s head of contracting activity.

“(B) RULE OF CONSTRUCTION.—None of the authorities authorized in this subsection shall prohibit the Chief Procurement Officer from retaining contracting authority for the Agency, as warranted.

“(5) COMPLIANCE.—The Agency shall comply with Department policy prior to obligating funds when using reimbursable work agreements or inter-agency acquisitions with other Federal agencies or Department components.

“(6) DEPARTMENT REVIEW.—Not later than one year after any delegation pursuant to paragraph (3), the Director shall report to Congress on the exercise of procurement and contracting authority by the head of contracting activity of the Agency and the status of Agency major acquisition programs, cost, schedule, and performance.

“(k) STAFF.—

“(1) IN GENERAL.—The Secretary shall provide the Agency with a staff of analysts having appro-
priate expertise and experience to assist the Agency in discharging its responsibilities under this section.

“(2) Private sector analysts.—Analysts under this subsection may include analysts from the private sector.

“(3) Security clearances.—Analysts under this subsection shall possess security clearances appropriate for their work under this section.

“(1) Detail of personnel.—

“(1) In general.—In order to assist the Agency in discharging its responsibilities under this section, personnel of the Federal agencies referred to in paragraph (2) may be detailed to the Agency for the performance of analytic functions and related duties.

“(2) Agencies specified.—The Federal agencies referred to in paragraph (1) are the following:

“(A) The Department of State.

“(B) The Central Intelligence Agency.

“(C) The Federal Bureau of Investigation.

“(D) The National Security Agency.

“(E) The National Geospatial-Intelligence Agency.

“(F) The Defense Intelligence Agency.
“(G) Any other agency of the Federal Government that the President considers appropriate.

“(3) COOPERATIVE AGREEMENTS.—The Secretary and the head of the agency concerned under this subsection may enter into cooperative agreements for the purpose of detailing personnel under this subsection.

“(4) BASIS.—The detail of personnel under this subsection may be on a reimbursable or non-reimbursable basis.

“SEC. 2203. CYBERSECURITY DIVISION.

“(a) ESTABLISHMENT.—

“(1) IN GENERAL.—There is established in the Agency a Cybersecurity Division.

“(2) PRINCIPAL DEPUTY DIRECTOR.—The Cybersecurity Division shall be headed by a Principal Deputy Director of Cybersecurity (in this subtitle referred to as the ‘Principal Deputy Director’), who shall—

“(A) be at the level of Assistant Secretary within the Department; and

“(B) report to the Director.

“(3) REFERENCE.—Any reference to the Assistant Secretary for Cybersecurity and Communications—
tions in any law, regulation, map, document, record, or other paper of the United States shall be deemed to be a reference to Principal Deputy Director of Cybersecurity.

“(b) FUNCTIONS.—The Cybersecurity Division shall—

“(1) lead the cybersecurity efforts of the Agency;

“(2) carry out—

“(A) the Department’s activities related to Federal information security; and

“(B) the functions of the national cybersecurity and communications integration center under section 2209;

“(3) coordinate cybersecurity initiatives with Federal and non-Federal entities for all activities relating to stakeholder outreach, engagement, and education, including engagement and coordination activities for cybersecurity initiatives carried out by the National Protection and Programs Directorate, Office of Cybersecurity and Communications Stakeholder Engagement and Cyber Infrastructure Resilience division as of June 1, 2015;
“(4) provide coordination and support to non-
Federal entities to reduce cybersecurity risks, includ-
ing through voluntary partnerships;

“(5) conduct network and malicious code anal-
ysis for known and unknown cybersecurity threats; and

“(6) in coordination with the Director, carry out the consultation, coordination, and collaboration required under subsection (d)(4) of section 2202.

“(c) ADDITIONAL FUNCTIONS.—In addition to the responsibilities specified in subsection (b), the Principal Deputy Director shall also—

“(1) under section 201, carry out paragraphs (1), (3), (4), (5), (6), (8), (10), (11), (13), (14), and (22) of subsection (d) of such section;

“(2) carry out comprehensive assessments of the cybersecurity risks to critical infrastructure, including the performance of risk assessments to determine the risks posed by particular types of terrorist attacks within the United States (including an assessment of the probability of success of such attacks and the feasibility and potential efficacy of various countermeasures to such attacks);

“(3) recommend cybersecurity measures nec-
ecessary to protect critical infrastructure in coordina-
tion with other Federal entities and in cooperation
with non-Federal entities; and
“(4) ensure that any material received pursuant
to this title is protected from unauthorized disclo-
sure and handled and used only for the performance
of official duties.

“SEC. 2204. INFRASTRUCTURE PROTECTION DIVISION.

“(a) Establishment.—
“(1) In general.—There is established in the
Agency an Infrastructure Protection Division.
“(2) Deputy Director.—The Infrastructure
Protection Division shall be headed by a Deputy Di-
rector of Infrastructure Protection (in this section
referred to as the ‘Deputy Director’), who shall re-
port to the Director.
“(3) Reference.—Any reference to the Assistant
Secretary for Infrastructure Protection in any
law, regulation, map, document, record, or other
paper of the United States shall be deemed to be a
reference to Deputy Director of Infrastructure Pro-
tection.
“(b) Functions.—The Infrastructure Protection Di-
vision shall—
“(1) lead the critical infrastructure protection
efforts of the Agency;
“(2) gather and manage critical infrastructure information and ensure that such information is available to the leadership of the Department and critical infrastructure owners and operators;

“(3) lead the efforts of the Department to secure the United States high-risk chemical facilities, including the Chemical Facilities Anti-Terrorism Standards established under title XXI;

“(4) provide coordination and support to non-Federal entities to reduce risk to critical infrastructure from terrorist attack or natural disaster, including through voluntary partnerships;

“(5) operate stakeholder engagement mechanisms for appropriate critical infrastructure sectors, except that such mechanisms may not duplicate any engagement and coordination activities for cybersecurity initiatives carried out by the National Protection and Programs Directorate, Office of Cybersecurity and Communications Stakeholder Engagement and Cyber Infrastructure Resilience division as of June 1, 2015;

“(6) administer the Coordinating Center established under subsection (d);
“(7) in coordination with the Director, carry out the consultation and collaboration required under subsection (d)(4) of section 2202; and

“(8) carry out such other duties and powers as prescribed by the Director.

“(c) ADDITIONAL FUNCTIONS.—In addition to the responsibilities specified in subsection (b), the Deputy Director shall also—

“(1) under section 201, carry out paragraphs (1), (3), (4), (5), (6), (8), (10), (11), (13), (14), and (22) subsection (d) of such section;

“(2) carry out comprehensive assessments of the vulnerabilities of critical infrastructure, including the performance of risk assessments to determine the risks posed by particular types of terrorist attacks within the United States (including an assessment of the probability of success of such attacks and the feasibility and potential efficacy of various countermeasures to such attacks);

“(3) recommend measures necessary to protect critical infrastructure in coordination with other Federal entities and in cooperation with non-Federal entities; and

“(4) ensure that any material received pursuant to this title is protected from unauthorized disclo-
sure and handled and used only for the performance
of official duties.

“(d) COORDINATING CENTER.—There shall be within
the Infrastructure Protection Division a National Infra-
structure Coordinating Center which shall be headed by
an Assistant Director and be co-located with the national
cybersecurity communications and integrated center estab-
lished under section 2209. The National Infrastructure
Coordinating Center shall—

“(1) collect, maintain, and share critical infra-
structure information;

“(2) evaluate critical infrastructure information
for accuracy, importance, and implications;

“(3) provide recommendations to non-Federal
entities and Department leadership;

“(4) advise the Secretary and the Director re-
garding actions required before and after a critical
infrastructure incident; and

“(5) carry out such other duties and powers as
prescribed by the Director.”.

(b) TREATMENT OF CERTAIN POSITIONS.—

(1) UNDER SECRETARY.—The individual serv-
ing as the Under Secretary appointed pursuant to
section 103(a)(1)(H) of the Homeland Security Act
of 2002 (6 U.S.C. 113(a)(1)) of the Department of
Homeland Security on the day before the date of the enactment of this Act may continue to serve as the Director of the Cybersecurity and Infrastructure Protection Agency of the Department on and after such date.

(2) Director for Emergency Communications.—The individual serving as the Director for Emergency Communications of the Department of Homeland Security on the day before the date of the enactment of this Act may continue to serve as the Deputy Director of Emergency Communications of the Department on and after such date.

(3) Assistant Secretary for Cybersecurity and Communications.—The individual serving as the Assistant Secretary for Cybersecurity and Communications on the day before the date of the enactment of this Act may continue to serve as the Principal Deputy Director of Cybersecurity.

(4) Assistant Secretary for Infrastructure Protection.—The individual serving as the Assistant Secretary for Infrastructure Protection on the day before the date of the enactment of this Act may continue to serve as the Deputy Director of Infrastructure Protection.
(c) **OPERATIONAL COORDINATION.**—The Director of the Cybersecurity and Infrastructure Protection Agency of the Department of Homeland Security shall provide, in accordance with the deadlines specified in paragraphs (1) and (2), to the Committee on Homeland Security of the House and the Committee on Homeland Security and Governmental Affairs of the Senate information on the following:

(1) Not later than 90 days after the date of the enactment of this Act, the Agency’s mechanisms for regular consultation and collaboration, including information on composition (including leadership structure), authorities, frequency of meetings, and visibility within the Agency.

(2) Not later than one year after the date of the enactment of this Act, the activities of the Agency’s consultation and collaboration mechanisms and how such mechanisms have impacted operational coordination, situational awareness, and integration across the Agency.

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

(1) in section 103(a) (6 U.S.C. 113(a))—

(A) in paragraph (1), by amending sub-paragraphs (H) and (I) to read as follows:
“(H) A Director of the Cybersecurity and Infrastructure Protection Agency.

“(I) The Administrator of the Transportation Security Administration.”; and

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

“(2) Other Assistant Secretaries and Officials.—

“(A) Presidential appointments.—The Department shall have the following officers appointed by the President:

“(i) The Principal Deputy Director of the Cybersecurity Division under section 2203.

“(ii) The Assistant Secretary of the Office of Public Affairs.

“(iii) The Assistant Secretary of the Office of Legislative Affairs.

“(B) Secretarial appointments.—The Department shall have the following Assistant Secretaries appointed by the Secretary:

“(i) The Assistant Secretary for International Affairs under section 602.

“(ii) The Assistant Secretary for Partnership and Engagement under section 603.
“(C) LIMITATION ON CREATION OF POSITIONS.—No Assistant Secretary position may be created in addition to the positions provided for by this section unless such position is authorized by a statute enacted after the date of the enactment of the Cybersecurity and Infrastructure Protection Agency Act of 2016.”;

(2) in title II (6 U.S.C. 121 et seq.)—

(A) in the title heading, by striking “AND INFRASTRUCTURE PROTECTION”;

(B) in the subtitle A heading, by striking “and Infrastructure Protection; Access to Information”;

(C) in section 201 (6 U.S.C. 121)—

(i) in the section heading, by striking “AND INFRASTRUCTURE PROTECTION”;

(ii) in subsection (a)—

(I) in the heading, by striking “AND INFRASTRUCTURE PROTECTION”; and

(II) by striking “and an Office of Infrastructure Protection”;

(iii) in subsection (b)—
(I) in the heading, by striking “AND ASSISTANT SECRETARY FOR INFRASTRUCTURE PROTECTION”; and

(II) by striking paragraph (3);

(iv) in subsection (c)—

(I) by striking “and infrastructure protection”; and

(II) by striking “or the Assistant Secretary for Infrastructure Protection, as appropriate”;

(v) in subsection (d)—

(I) in the heading, by striking “AND INFRASTRUCTURE PROTECTION”;  

(II) in the matter preceding paragraph (1), by striking “and infrastructure protection”;  

(III) by striking paragraphs (5) and (6) and redesignating paragraphs (7) through (25) as paragraphs (4) through (23), respectively; and

(IV) by striking paragraph (23), as so redesignated;
(vi) in subsection (e)(1), by striking “and the Office of Infrastructure Protec-
tion”; and
(vii) in subsection (f)(1), by striking “and the Office of Infrastructure Protec-
tion”;
(D) by redesignating sections 223 through 230 (6 U.S.C. 143–151) as sections 2205 through 2212, respectively, and inserting such redesignated sections after section 2204, as added by this title;
(E) by redesignating section 210E (6 U.S.C. 124) as section 2213 and inserting such redesignated section after section 2212; and
(F) in subtitle B, by redesignating sections 211 through 215 (6 U.S.C. 101 note through 134) as sections 2214 through 2218, respectively, and inserting such redesignated sections, including the subtitle B designation (including the enumerator and heading), after section 2213;
(3) in title XVIII (6 U.S.C. 571 et seq.)—
(A) in section 1801 (6 U.S.C. 571)—
   (i) in the section heading, by striking “OFFICE OF EMERGENCY COMMU-
NICATIONS” and inserting “EMERGENCY COMMUNICATIONS DIVISION”;

(ii) in subsection (a)—

(I) by striking “Office of Emergency Communications” and inserting “Emergency Communications Division”; and

(II) by adding at the end the following new sentence: “The Division shall be located in the Cybersecurity and Infrastructure Protection Agency.”; and

(iii) in subsection (b)—

(I) in the first sentence, by striking “Director for” and inserting “Deputy Director of”; and

(II) in the second sentence, by striking “Assistant Secretary for Cybersecurity and Communications” and inserting “Director of the Cybersecurity and Infrastructure Protection Agency”; and

(III) in subsection (e)—

(aa) in the matter preceding paragraph (1), by striking “Di-
rector for” and inserting “Deputy Director of”;

(bb) by redesignating paragraphs (1) and (2) as paragraphs (2) and (3), respectively; and

(cc) by inserting before paragraph (2), as so redesignated, the following new paragraph:

“(1) with the Director of the Cybersecurity and Infrastructure Protection Agency to carry out the consultation and collaboration required under subsection (d)(4) of section 2202;”;

(B) in sections 1801 through 1805 (6 U.S.C. 575), by striking “Director for Emergency Communications” each place it appears and inserting “Deputy Director of Emergency Communications”;

(C) in section 1809 (6 U.S.C. 579)—

(i) by striking “Director for Emergency Communications” each place it appears and inserting “Deputy Director of Emergency Communications”; and

(ii) by striking “Office of Emergency Communications” each place it appears
and inserting “Emergency Communications Division”; and

(D) in section 1810 (6 U.S.C. 580)—

(i) by striking “Director” each place it appears and inserting “Deputy Director”; 

(ii) by striking “Office of Emergency Communications” each place it appears and inserting “Emergency Communications Division”; and 

(iii) in subsection (a)(1), by striking “Director of the Office of Emergency Communications (referred to in this section as the ‘Director’)” and inserting “Deputy Director of the Emergency Communications Division (referred to in this section as the ‘Deputy Director’)”; 

(4) in title XXI (6 U.S.C. 621 et seq.)—

(A) in section 2101 (6 U.S.C. 621)—

(i) by redesignating paragraphs (4) through (14) as paragraphs (5) through (15), respectively;

(ii) by inserting after paragraph (3) the following new paragraph:
“(4) the term ‘Director’ means the Director of the Cybersecurity and Infrastructure Protection Agency;”;

(iii) by further redesignating paragraphs (11) through (15) (as redesignated pursuant to clause (i)) as paragraphs (12) through (16); and

(iv) by inserting after paragraph (10) (as redesignated pursuant to clause (i)) the following new paragraph:

“(11) the term ‘Secretary’ means the Secretary acting through the Director;”;

(B) in paragraph (1) of section 2102(a) (6 U.S.C. 622(a)), by inserting at the end the following new sentence: “Such Programs shall be located in the Cybersecurity and Infrastructure Protection Agency.”; and

(C) in paragraph (2) of section 2104(c) (6 U.S.C. 624(e)), by striking “Under Secretary responsible for overseeing critical infrastructure protection, cybersecurity, and other related programs of the Department appointed under section 103(a)(1)(H)” and inserting “Director of the Cybersecurity and Infrastructure Protection Agency”; and
(5) in title XXII, as added by this title—

(A) in section 2205, as so redesignated, in the matter preceding paragraph (1), by striking “Under Secretary appointed under section 103(a)(1)(H)” and inserting “Director of the Cybersecurity and Infrastructure Protection Agency”;

(B) in section 2209, as so redesignated—

(i) by striking “Under Secretary appointed under section 103(a)(1)(H)” each place it appears and inserting “Director of the Cybersecurity and Infrastructure Protection Agency”;

(ii) in subsection (b), by adding at the end the following new sentences: “The Center shall be located in the Cybersecurity and Infrastructure Protection Agency. The head of the Center shall be an Assistant Director of the Center, who shall report to the Principal Deputy Director for Cybersecurity.”; and

(iii) in subsection (c), by striking “Office of Emergency Communications” and inserting “Emergency Communications Division”;
(C) in section 2210, as so redesignated—

   (i) by striking “section 227” each place it appears and inserting “section 2209”; and

   (ii) in subsection (e), by striking “Under Secretary appointed under section 103(a)(1)(H)” and inserting “Director of the Cybersecurity and Infrastructure Protection Agency”;

(D) in section 2211, as so redesignated, by striking “section 212(5)” and inserting “section 2215(5)”;

(E) in section 2212, as so redesignated, in subsection (a)—

   (i) in paragraph (3), by striking “section 228” and inserting “section 2210”; and

   (ii) in paragraph (4), by striking “section 227” and inserting “section 2209”.

(e) Clerical Amendment.—The table of contents in section 1(b) of the Homeland Security Act of 2002 is amended—

   (1) by striking the item relating to section 210E;
(2) by striking the items relating to section 211 through section 215, including the subtitle B designation (including the enumerator and heading);

(3) by striking the items relating to section 223 through section 230; and

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

"TITLE XXII—CYBERSECURITY AND INFRASTRUCTURE PROTECTION AGENCY

Subtitle A—Cybersecurity and Infrastructure Protection

Sec. 2201. Definitions.
Sec. 2202. Cybersecurity and Infrastructure Protection Agency.
Sec. 2203. Cybersecurity Division.
Sec. 2204. Infrastructure Protection Division.
Sec. 2206. Net guard.
Sec. 2208. Cybersecurity recruitment and retention.
Sec. 2209. National cybersecurity and communications integration center.
Sec. 2210. Cybersecurity plans.
Sec. 2211. Clearances.
Sec. 2212. Federal intrusion detection and prevention system.
Sec. 2213. National Asset Database.

Subtitle B—Critical Infrastructure Information

Sec. 2214. Short title.
Sec. 2215. Definitions.
Sec. 2216. Designation of critical infrastructure protection program.
Sec. 2217. Protection of voluntarily shared critical infrastructure information.
Sec. 2218. No private right of action.”.

SEC. 602. ESTABLISHMENT OF THE OFFICE OF BIOMETRIC IDENTITY MANAGEMENT.

(a) IN GENERAL.—Title VII of the Homeland Security Act of 2002 (6 U.S.C. 341, et seq.) is amended by adding at the end the following new section:
“SEC. 708. OFFICE OF BIOMETRIC IDENTITY MANAGEMENT.

“(a) Establishment.—The Office of Biometric Identity Management is established within the Department.

“(b) Director.—

“(1) In General.—The Office of Biometric Identity Management shall be administered by the Director of the Office of Biometric Identity Management (in this section referred to as the ‘Director’) who shall report to the Under Secretary for Management, or to another official of the Department, as the Under Secretary for Management may direct.

“(2) Qualifications and Duties.—The Director shall—

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

“(B) lead the Department’s biometric identity services to support anti-terrorism, counter-terrorism, border security, credentialing, national security, and public safety, and enable operational missions across the Department by matching, storing, sharing, and analyzing biometric data;

“(C) deliver biometric identity information and analysis capabilities to—
“(i) the Department and its components;

“(ii) appropriate Federal, State, local, territorial, and tribal agencies;

“(iii) appropriate foreign governments; and

“(iv) appropriate private sector entities;

“(D) support the law enforcement, public safety, national security, and homeland security missions of other Federal, State, local, territorial, and tribal agencies, as appropriate;

“(E) establish and manage the operation and maintenance of the Department’s sole biometric repository;

“(F) establish, manage, and operate Biometric Support Centers to provide biometric identification and verification analysis and services to the Department, appropriate Federal, State, local, territorial, and tribal agencies, appropriate foreign governments, and appropriate private sector entities;

“(G) in collaboration with the Undersecretary for Science and Technology, establish a Department-wide research and development
program to support efforts in assessment, development, and exploration of biometric advancements and emerging technologies;

“(H) oversee Department-wide standards for biometric conformity, and work to make such standards Government-wide;

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

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

“(K) carry out the duties and powers prescribed by law or delegated by the Secretary.

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

“(d) CHIEF TECHNOLOGY OFFICER.—
“(1) IN GENERAL.—There shall be in the Office of Biometric Identity Management a Chief Technology Officer.

“(2) DUTIES.—The Chief Technology Officer shall—

“(A) ensure compliance with policies, processes, standards, guidelines, and procedures related to information technology systems management, enterprise architecture, and data management;

“(B) provide engineering and enterprise architecture guidance and direction to the Office of Biometric Identity Management; and

“(C) leverage emerging biometric technologies to recommend improvements to major enterprise applications, identify tools to optimize information technology systems performance, and develop and promote joint technology solutions to improve services to enhance mission effectiveness.

“(e) OTHER AUTHORITIES.—

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

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

(b) Transfer Limitation.—The Secretary of Homeland Security may not transfer the location or reporting structure of the Office of Biometric Identity Management (established by section 708 of the Homeland Security Act of 2002, as added by subsection (a) of this section) to any component of the Department of Homeland Security.

(c) Clerical Amendment.—The table of contents in section 1(b) of the Homeland Security Act of 2002 is amended by adding after the item relating to section 707 the following new item:

“Sec. 708. Office of Biometric Identity Management.”.

SEC. 603. RULE OF CONSTRUCTION.

Nothing in this title may be construed to confer new authorities to the Secretary of Homeland Security, including programmatic and regulatory authorities, outside of
the authorities that existed on the day before the date of
the enactment of this Act.

SEC. 604. PROHIBITION ON ADDITIONAL FUNDING.
No additional funds are authorized to be appro-
priated to carry out this title or the amendments made
by this title.

TITLE VII—STRENGTHENING CY-
BERSECURITY INFORMATION
SHARING AND COORDINA-
TION IN OUR PORT

SEC. 701. IMPROVING CYBERSECURITY RISK ASSESSMENTS,
INFORMATION SHARING, AND COORDINA-
TION.
The Secretary of Homeland Security shall—
(1) develop and implement a maritime cyberse-
curity risk assessment model within 120 days after
the date of the enactment of this Act, consistent
with the National Institute of Standards and Tech-
ology Framework for Improving Critical Infrastruc-
ture Cybersecurity and any update to that document
pursuant to Public Law 113–274, to evaluate cur-
rent and future cybersecurity risks (as that term is
defined in the second section 226 of the Homeland
(2) evaluate, on a periodic basis but not less than once every two years, the effectiveness of the cybersecurity risk assessment model established under paragraph (1);

(3) seek to ensure participation of at least one information sharing and analysis organization (as that term is defined in section 212 of the Homeland Security Act of 2002 (6 U.S.C. 131)) representing the maritime community in the National Cybersecurity and Communications Integration Center, pursuant to subsection (d)(1)(B) of the second section 226 of the Homeland Security Act of 2002 (6 U.S.C. 148);

(4) establish guidelines for voluntary reporting of maritime-related cybersecurity risks and incidents (as such terms are defined in the second section 226 of the Homeland Security Act of 2002 (6 U.S.C. 148)) to the Center (as that term is defined subsection (b) of the second section 226 of the Homeland Security Act of 2002 (6 U.S.C. 148)), and other appropriate Federal agencies; and

(5) request the National Maritime Security Advisory Committee established under section 70112 of title 46, United States Code, to report and make recommendations to the Secretary on enhancing the
sharing of information related to cybersecurity risks and incidents between relevant Federal agencies and State, local, and tribal governments and consistent with the responsibilities of the Center (as that term is defined subsection (b) of the second section 226 of the Homeland Security Act of 2002 (6 U.S.C. 148)); relevant public safety and emergency response agencies; relevant law enforcement and security organizations; maritime industry; port owners and operators; and terminal owners and operators.

SEC. 702. CYBERSECURITY ENHANCEMENTS TO MARITIME SECURITY ACTIVITIES.

The Secretary of Homeland Security, acting through the Commandant of the Coast Guard, shall direct—

(1) each Area Maritime Security Advisory Committee established under section 70112 of title 46, United States Code, to facilitate the sharing of cybersecurity risks and incidents to address port-specific cybersecurity risks, which may include the establishment of a working group of members of Area Maritime Security Advisory Committees to address port-specific cybersecurity vulnerabilities; and

(2) that any area maritime security plan and facility security plan required under section 70103 of title 46, United States Code approved after the
development of the cybersecurity risk assessment
model required by paragraph (1) of section 801 in-
clude a mitigation plan to prevent, manage, and re-
spond to cybersecurity risks.

SEC. 703. VULNERABILITY ASSESSMENTS AND SECURITY PLANS.

Title 46, United States Code, is amended—

(1) in section 70102(b)(1)(C), by inserting “cy-
bersecurity,” after “physical security,”; and

(2) in section 70103(c)(3)(C), by striking “and” after the semicolon at the end of clause (iv),
by redesignating clause (v) as clause (vi), and by in-
serting after clause (iv) the following:

“(v) prevention, management, and re-
sponse to cybersecurity risks; and”.

TITLE VIII—STRENGTHENING STATE AND LOCAL CYBER CRIME FIGHTING

SEC. 801. AUTHORIZATION OF THE NATIONAL COMPUTER FORENSICS INSTITUTE OF THE DEPARTMENT OF HOMELAND SECURITY.

(a) In General.—Subtitle C of title VIII of the Homeland Security Act of 2002 (6 U.S.C. 381 et seq.) is amended by adding at the end the following new section:
SEC. 822. NATIONAL COMPUTER FORENSICS INSTITUTE.

“(a) In General.—There is established in the Department a National Computer Forensics Institute (in this section referred to as the ‘Institute’), to be operated by the United States Secret Service, for the dissemination of homeland security information related to the investigation and prevention of cyber and electronic crime and related threats to educate, train, and equip State, local, tribal, and territorial law enforcement officers, prosecutors, and judges.

“(b) Functions.—The functions of the Institute shall include the following:

“(1) Educating State, local, tribal, and territorial law enforcement officers, prosecutors, and judges on current—

“(A) cyber and electronic crimes and related threats;

“(B) methods for investigating cyber and electronic crime and related threats and conducting computer and mobile device forensic examinations; and

“(C) prosecutorial and judicial challenges related to cyber and electronic crime and related threats, and computer and mobile device forensic examinations.
“(2) Training State, local, tribal, and territorial law enforcement officers to—

“(A) conduct cyber and electronic crime and related threat investigations;

“(B) conduct computer and mobile device forensic examinations; and

“(C) respond to network intrusion incidents.

“(3) Training State, local, tribal, and territorial law enforcement officers, prosecutors, and judges on methods to obtain, process, store, and admit digital evidence in court.

“(c) PRINCIPLES.—In carrying out the functions under subsection (b), the Institute shall ensure, to the extent practicable, that timely, actionable, and relevant expertise and homeland security information related to cyber and electronic crime and related threats is shared with State, local, tribal, and territorial law enforcement officers, prosecutors, and judges.

“(d) EQUIPMENT.—The Institute is authorized to provide State, local, tribal, and territorial law enforcement officers, prosecutors, and judges with computer equipment, hardware, software, manuals, and tools necessary to conduct cyber and electronic crime and related threats.
investigations and computer and mobile device forensic examinations.

“(e) **Electronic Crime Task Forces.**—The Institute shall facilitate the expansion of the Secret Service’s network of Electronic Crime Task Forces through the addition of task force officers of State, local, tribal, and territorial law enforcement officers, prosecutors, and judges educated and trained at the Institute, in addition to academia and private sector stakeholders.

“(f) **Coordination With Federal Law Enforcement Training Center.**—The Institute shall seek opportunities to coordinate with the Federal Law Enforcement Training Center within the Department to help enhance, to the extent practicable, the training provided by the Center to stakeholders, including by helping to ensure that such training reflects timely, actionable, and relevant expertise in homeland security information related to cyber and electronic crime and related threats.”.

(b) **No Additional Funding.**—No additional funds are authorized to be appropriated to carry out this title and the amendment made by this title. This title and such amendment shall be carried out using amounts otherwise available for such purposes.

(c) **Clerical Amendment.**—The table of contents of the Homeland Security Act of 2002 is amended by in-
serting after the item relating to section 821 the following new item:

“Sec. 822. National Computer Forensics Institute.”.

TITLE IX—DEPARTMENT OF HOMELAND SECURITY CBRNE DEFENSE

SEC. 901. CBRNE OFFICE.

(a) In General.—The Homeland Security Act of 2002 is amended by adding at the end the following new title:

“TITLE XXII—CBRNE OFFICE

Subtitle A—Chemical, Biological, Radiological, Nuclear, and Explosives Office

SEC. 2201. CHEMICAL, BIOLOGICAL, RADIOLOGICAL, NUCLEAR, AND EXPLOSIVES OFFICE.

“(a) Establishment.—There is established in the Department a Chemical, Biological, Radiological, Nuclear, and Explosives Office (referred to in this title as the ‘CBRNE Office’). The CBRNE Office shall be comprised of the Chemical Division, the Biological Division, the Nuclear Division, and the Explosives Division. The CBRNE Office may include a Health Division.

“(b) Mission of Office.—The mission of the CBRNE Office is to coordinate, strengthen, and provide
chemical, biological, radiological, nuclear, and explosives (CBRNE) capabilities in support of homeland security.

“(c) ASSISTANT SECRETARY.—The Office shall be headed by an Assistant Secretary for the Chemical, Biological, Radiological, Nuclear, and Explosives Office (referred to in this title as the ‘Assistant Secretary’), who shall be appointed by the President by and with the advice and consent of the Senate.

“(d) RESPONSIBILITIES.—The Assistant Secretary shall—

“(1) develop, coordinate, and maintain overall CBRNE strategy and policy for the Department;

“(2) develop, coordinate, and maintain for the Department periodic CBRNE risk assessments;

“(3) serve as the primary Department representative for coordinating CBRNE activities with other Federal departments and agencies;

“(4) provide oversight for the Department’s preparedness for CBRNE threats;

“(5) provide support for operations during CBRNE threats or incidents; and

“(6) carry out such other responsibilities as the Secretary determines appropriate, consistent with this title.
“(e) OTHER OFFICERS.—The Director of the Chemical Division, the Director of the Biological Division, the Director of the Nuclear Division, and the Director of the Explosives Division shall report directly to the Assistant Secretary.

“SEC. 2202. COMPOSITION OF THE CBRNE OFFICE.

“The Secretary shall transfer to the CBRNE Office, the functions, personnel, budget authority, and assets of the following:

“(1) The Office of Health Affairs as in existence on the day before the date of the enactment of this title, including the Chief Medical Officer authorized under section 516, and the National Biosurveillance Integration Center authorized under section 316.

“(2) The Domestic Nuclear Detection Office authorized under title XIX, as in existence on the date before the date of the enactment of this title (and redesignated as the Nuclear Division).

“(3) CBRNE threat awareness and risk assessment activities of the Science and Technology Directorate.

“(5) The Office for Bombing Prevention of the National Protection and Programs Directorate, as in existence on the day before the date of the enactment of this title.

“SEC. 2203. HIRING AUTHORITY.

“In hiring personnel for the CBRNE Office, the Secretary shall have the hiring and management authorities provided in section 1101 of the Strom Thurmond National Defense Authorization Act for Fiscal Year 1999 (5 U.S.C. 3104 note; Public Law 105–261), except that the term of appointments for employees under subsection (c)(1) of such section may not exceed 5 years before granting any extension under subsection (c)(2) of such section.

“SEC. 2204. GRANTS, COOPERATIVE AGREEMENTS, AND OTHER TRANSACTIONS AND CONTRACTS.

“The Assistant Secretary, in carrying out the responsibilities under this title, may distribute funds through grants, cooperative agreements, and other transactions and contracts.

“SEC. 2205. TERRORISM RISK ASSESSMENTS.

“(a) TERRORISM RISK ASSESSMENTS.—

“(1) IN GENERAL.—The Assistant Secretary shall, in coordination with relevant Department components and other appropriate Federal departments and agencies, develop, coordinate, and update peri-
odically terrorism risk assessments of chemical, biological, radiological, and nuclear threats.

“(2) COMPARISON.—The Assistant Secretary shall develop, coordinate, and update periodically an integrated terrorism risk assessment that assesses all of the threats referred to in paragraph (1) and, as appropriate, explosives threats, and compares each such threat against one another according to their relative risk.

“(3) INCLUSION IN ASSESSMENT.—Each terrorism risk assessment under this subsection shall include a description of the methodology used for each such assessment.

“(4) UPDATES.—Each terrorism risk assessment under this subsection shall be updated not less often than once every 2 years.

“(5) PROVISION TO CONGRESS.—The Assistant Secretary shall provide a copy of each risk assessment under this subsection to the Committee on Homeland Security of the House of Representatives and the Committee on Homeland Security and Governmental Affairs of the Senate not later than 30 days after completion of each such assessment.

“(b) METHODOLOGY.—In developing the terrorism risk assessments under subsection (a), the Assistant Sec-
Secretary, in consultation with appropriate Federal departments and agencies, shall—

“(1) assess the proposed methodology to be used for such assessments; and

“(2) consider the evolving threat to the United States as indicated by the intelligence community (as such term is defined in section 3(4) of the National Security Act of 1947 (50 U.S.C. 3003(4))).

“(c) USAGE.—The terrorism risk assessments required under subsection (a) shall be used to inform and guide allocation of resources for chemical, biological, radiological, and nuclear threat activities of the Department.

“(d) INPUT AND SHARING.—The Assistant Secretary shall, for each terrorism risk assessment under subsection (a)—

“(1) seek input from national stakeholders and other Federal, State, local, tribal, and territorial officials involved in efforts to counter chemical, biological, radiological, and nuclear threats;

“(2) ensure that written procedures are in place to guide the development of such assessments, including for input, review, and implementation purposes, among relevant Federal partners;

“(3) share such assessments with Federal, State, local, tribal, and territorial officials with ap-
propriate security clearances and a need for the information in the classified versions of such assessments; and

“(4) to the maximum extent practicable, make available an unclassified version of such assessments for Federal, State, local, tribal, and territorial officials involved in prevention and preparedness for chemical, biological, radiological, and nuclear events.

“SEC. 2206. CBRNE COMMUNICATIONS AND PUBLIC MESSAGING.

“(a) In General.—The Secretary, in coordination with the Assistant Secretary, shall develop an overarching risk communication strategy for terrorist attacks and other high consequence events utilizing chemical, biological, radiological, or nuclear agents or explosives that pose a high risk to homeland security, and shall—

“(1) develop threat-specific risk communication plans, in coordination with appropriate Federal departments and agencies;

“(2) develop risk communication messages, including pre-scripted messaging to the extent practicable;

“(3) develop clearly defined interagency processes and protocols to assure coordinated risk and
incident communications and information sharing during incident response;

“(4) engage private and nongovernmental entities in communications planning, as appropriate;

“(5) identify ways to educate and engage the public about CBRNE threats and consequences;

“(6) develop strategies for communicating using social and new media; and

“(7) provide guidance on risk and incident communications for CBRNE events to State, local, tribal, and territorial governments, and other stakeholders, as appropriate.

“(b) COMMUNICATION DURING RESPONSE.—The Secretary shall provide appropriate timely, accurate information to the public, governmental partners, the private sector, and other appropriate stakeholders in the event of a suspected or confirmed terrorist attack or other high consequence event utilizing chemical, biological, radiological, or nuclear agents or explosives that pose a high risk to homeland security.

“(c) REPORTS.—

“(1) DEVELOPMENT EFFORTS.—Not later than 120 days after the date of the enactment of this title, the Secretary shall submit to the Committee on Homeland Security of the House of Representatives...
and the Committee on Homeland Security and Governmental Affairs of the Senate a report on current and future efforts of the Department to develop the communication strategy required under subsection (a).

“(2) Finalization.—Not later than 2 years after the date the report required under paragraph (1) is submitted, the Secretary shall submit to the Committee on Homeland Security of the House of Representatives and the Committee on Homeland Security and Governmental Affairs of the Senate the communication strategy required under subsection (a).

“SEC. 2207. CHEMICAL, BIOLOGICAL, RADIOLOGICAL, NUCLEAR, AND EXPLOSIVES INTELLIGENCE AND INFORMATION SHARING.

“(a) In General.—The Under Secretary of Intelligence and Analysis of the Department shall—

“(1) support homeland security-focused intelligence analysis of terrorist actors, their claims, and their plans to conduct attacks involving chemical, biological, radiological, or nuclear materials or explosives against the United States;
“(2) support homeland security-focused intelligence analysis of global infectious diseases, public health, food, agricultural, and veterinary issues;

“(3) support homeland security-focused risk analysis and risk assessments of the homeland security hazards described in paragraphs (1) and (2) by providing relevant quantitative and nonquantitative threat information;

“(4) leverage existing and emerging homeland security intelligence capabilities and structures to enhance prevention, protection, response, and recovery efforts with respect to a chemical, biological, radiological, nuclear, or explosives attack;

“(5) share appropriate information regarding such threats to appropriate State, local, tribal, and territorial authorities, as well as other national biodefense stakeholders; and

“(6) perform other responsibilities, as assigned by the Secretary.

“(b) COORDINATION.—Where appropriate, the Under Secretary of Intelligence and Analysis shall coordinate with the heads of other relevant Department components, including the Assistant Secretary, members of the intelligence community, including the National Counter Proliferation Center and the National Counterterrorism Cen-
ter, and other Federal, State, local, tribal, and territorial authorities, including officials from high-threat areas, to enable such entities to provide recommendations on optimal information sharing mechanisms, including expeditious sharing of classified information, and on how such entities can provide information to the Department.

“(c) REPORT.—

“(1) IN GENERAL.—Not later than 1 year after the date of the enactment of this section and annually thereafter for 5 years, the Secretary shall submit to the Committee on Homeland Security of the House of Representatives and the Committee on Homeland Security and Governmental Affairs of the Senate a report on—

“(A) the intelligence and information sharing activities under subsections (a) and (b) and of all relevant entities within the Department to prevent, protect against, prepare for, respond to, mitigate, and recover from terrorist attacks and other high consequence events utilizing chemical, biological, radiological, or nuclear agents or explosives that pose a high risk to homeland security; and

“(B) the Department’s activities in accordance with relevant intelligence strategies.
“(2) ASSESSMENT OF IMPLEMENTATION.—
Each report required under paragraph (1) shall also include—

“(A) a description of methods established to assess progress of the Office of Intelligence and Analysis in implementing this section; and

“(B) such assessment of such progress.

“(d) DEFINITIONS.—In this section:

“(1) INTELLIGENCE COMMUNITY.—The term ‘intelligence community’ has the meaning given such term in section 3(4) of the National Security Act of 1947 (50 U.S.C. 3003(4)).

“(2) NATIONAL BIOSECURITY AND BIODEFENSE STAKEHOLDERS.—The term ‘national biosecurity and biodefense stakeholders’ means officials from Federal, State, local, tribal, and territorial authorities and individuals from the private sector who are involved in efforts to prevent, protect against, prepare for, respond to, mitigate, and recover from a biological attack or other phenomena that may have serious health consequences for the United States, including infectious disease outbreaks.”.

(b) AFTER ACTION AND EFFICIENCIES REVIEW.—
Not later than 1 year after the date of the enactment of this Act, the Secretary of Homeland Security, acting
through the Assistant Secretary for the Chemical, Biological, Radiological, Nuclear, and Explosives Office of the Department of Homeland Security (established pursuant to section 2201 of the Homeland Security Act of 2002, as added by subsection (a) of this section), shall submit to the Committee on Homeland Security of the House of Representatives and the Committee on Homeland Security and Governmental Affairs of the Senate a report that—

(1) reviews the functions and responsibilities of the Chemical, Biological, Radiological, Nuclear, and Explosives Office of the Department (established pursuant to section 2201 of the Homeland Security Act of 2002, as added by subsection (a) of this section) to identify and eliminate areas of unnecessary duplication;

(2) provides a detailed accounting of the management and administrative expenditures and activities of the Office, including expenditures related to the establishment of the CBRNE Office, such as expenditures associated with the utilization of the Secretary’s authority to award retention bonuses pursuant to Federal law;

(3) identifies any potential cost savings and efficiencies within the CBRNE Office or its divisions; and
(4) identifies opportunities to enhance the effectiveness of the management and administration of the CBRNE Office to improve operational impact and enhance efficiencies.

(e) Chemical, Biological, Radiological, Nuclear, and Explosives Research and Development.—

(1) In general.—The Secretary of Homeland Security shall assess the organizational structure of the management and execution of the Department of Homeland Security’s chemical, biological, radiological, nuclear, and explosives research and development activities, and shall develop and submit to the Committee on Homeland Security, the Committee on Science, Space, and Technology, and the Committee on Appropriations of the House of Representatives and the Committee on Homeland Security and Governmental Affairs and the Committee on Appropriations of the Senate at the time the President submits the budget under section 1105 of title 31, United States Code, for the fiscal year that follows the issuance of the Comptroller General review required pursuant to subsection (d) a proposed organizational structure for the management and execution
of such chemical, biological, radiological, nuclear, and explosives research and development activities.

(2) ORGANIZATIONAL JUSTIFICATION.—The Secretary of Homeland Security shall include in the assessment required under paragraph (1) a thorough justification and rationalization for the proposed organizational structure for management and execution of chemical, biological, radiological, nuclear, and explosives research and development activities, including the following:

(A) A discussion of the methodology for determining such proposed organizational structure.

(B) A comprehensive inventory of chemical, biological, radiological, nuclear, and explosives research and development activities of the Department of Homeland Security and where each such activity will be located within or outside such proposed organizational structure.

(C) Information relating to how such proposed organizational structure will facilitate and promote coordination and requirements generation with customers.

(D) Information relating to how such proposed organizational structure will support the
development of chemical, biological, radiological, nuclear, and explosives research and development priorities across the Department.

(E) If the chemical, biological, radiological, nuclear, and explosives research and development activities of the Department are not co-located in such proposed organizational structure, a justification for such separation.

(F) The strategy for coordination between the Under Secretary for Science and Technology and the Assistant Secretary for the Chemical, Biological, Radiological, Nuclear, and Explosives Office on chemical, biological, radiological, nuclear, and explosives research and development activities.

(G) Recommendations for necessary statutory changes.

(3) LIMITATION ON ACTION.—The Secretary of Homeland Security may not take any action to reorganize the structure referred to in paragraph (1) unless the Secretary receives prior authorization from the Committee on Homeland Security and the Committee on Science, Space, and Technology of the House of Representatives and the Committee on
Homeland Security and Governmental Affairs of the Senate permitting any such action.

(d) GOVERNMENT ACCOUNTABILITY OFFICE REVIEW OF CHEMICAL, BIOLOGICAL, RADIOLOGICAL, NUCLEAR, AND EXPLOSIVES RESEARCH AND DEVELOPMENT ACTIVITIES.—

    (1) IN GENERAL.—The Comptroller General of the United States shall conduct a review of the organizational structure of the Department of Homeland Security’s management and execution of chemical, biological, radiological, nuclear, and explosives research and development activities.

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

        (A) An assessment of the organizational structure for the management and execution of chemical, biological, radiological, nuclear, and explosives research and development activities of the Department of Homeland Security, including identification of any overlap or duplication of effort.

        (B) Recommendations to streamline and improve the organizational structure of the Department’s management and execution of chem-
ical, biological, radiological, nuclear, and explosives research and development activities.

(3) Report.—Not later than 2 years after the date of the enactment of this Act, the Comptroller General shall submit to the Committee on Homeland Security and the Committee on Science, Space, and Technology of the House of Representatives and the Committee on Homeland Security and Governmental Affairs of the Senate a report on the review required under this subsection.

(e) Dissemination of Information Analyzed by the Department of Homeland Security to State, Local, Tribal, and Private Entities With Responsibilities Relating to Homeland Security.—Paragraph (8) of section 201(d) of the Homeland Security Act of 2002 (6 U.S.C. 121(d)) is amended by striking “and to agencies of State” and all that follows through the period at the end and inserting “to State, local, tribal, territorial, and appropriate private entities with such responsibilities, and, as appropriate, to the public, in order to assist in preventing, protecting against, preparing for, responding to, mitigating, and recovering from terrorist attacks against the United States.”.

(f) Technical and Conforming Amendments.—The Homeland Security Act of 2002 is amended—
(1) in paragraph (2) of section 103(a) (6 U.S.C. 113(a)), by striking “Assistant Secretary for Health Affairs, the Assistant Secretary for Legislative Affairs, or the Assistant Secretary for Public Affairs,” and inserting “Assistant Secretary for Legislative Affairs or the Assistant Secretary for Public Affairs,”;

(2) in section 302 (6 U.S.C. 182)—

(A) by redesignating paragraphs (13) and (14) as paragraphs (14) and (15), respectively;

and

(B) by inserting after paragraph (12) the following new paragraph:

“(13) collaborating with the Assistant Secretary for the Chemical, Biological, Radiological, Nuclear, and Explosives Office on all chemical, biological, and explosives research and development activities;”;

(3) in subsection (b) of section 307 (6 U.S.C. 187), by adding at the end the following new paragraph:

“(8) CBRNE DEFENSE.—The Director shall coordinate with the Assistant Secretary for the Chemical, Biological, Radiological, Nuclear, and Explosives Office on all chemical, biological, and explosives research and development activities.”; and
(4) in subsection (c) of section 516 (6 U.S.C. 321e)—

(A) in the matter preceding paragraph (1), by inserting “, including the health impacts of chemical, biological, radiological, and nuclear agents and explosives” after “natural disasters”;

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

“(2) coordinating the Department’s policy, strategy, and preparedness for pandemics and emerging infectious diseases;”; and

(C) in paragraph (6), by striking “Under Secretary for Science and Technology” and inserting “Assistant Secretary for the Chemical, Biological, Radiological, Nuclear, and Explosives Office”.

SEC. 902. CHEMICAL DIVISION.

(a) In General.—Title XXII of the Homeland Security Act of 2002, as added by section 901 of this title, is amended by adding at the end the following new sub-title:
“Subtitle B—Chemical Division

SEC. 2211. CHEMICAL DIVISION.

“(a) Establishment.—There is established in the CBRNE Office a Chemical Division, headed by a Director of the Chemical Division (in this subtitle referred to as the ‘Director’).

“(b) Mission and Responsibilities.—The Director shall be responsible for coordinating departmental strategy and policy relating to terrorist attacks and other high-consequence events utilizing chemical agents that pose a high risk to homeland security, including the following:

“(1) Developing and maintaining the Department’s strategy against chemical threats.

“(2) Serving as the Department representative for chemical threats and related activities with other Federal departments and agencies.

“(3) Providing oversight of the Department’s preparedness, including operational requirements, for chemical threats.

“(4) Enhancing the capabilities of Federal, State, local, tribal, and territorial governments, and private entities as appropriate, against chemical threats.
“(5) Evaluating and providing guidance to Federal, State, local, tribal, and territorial governments, and private entities as appropriate, on detection and communication technology that could be effective in terrorist attacks and other high-consequence events utilizing chemical agents.

“(6) Supporting and enhancing the effective sharing and use of appropriate information generated by the intelligence community (as such term is defined in section 3(4) of the National Security Act of 1947 (50 U.S.C. 3003(4))), law enforcement agencies, other Federal, State, local tribal, and territorial governments, and foreign governments, on chemical threats.

“SEC. 2212. DEMONSTRATION PROJECTS.

“(a) IN GENERAL.—The Director may, subject to the availability of appropriations for such purpose, partner with high-risk urban areas or facilities to conduct demonstration projects to enhance, through Federal, State, local, tribal, and territorial governments, and private entities, capabilities of the United States to counter terrorist attacks and other high-consequence events utilizing chemical agents that pose a high risk to homeland security.

“(b) GOALS.—The Director may provide guidance and evaluations for all situations and venues at risk of
terrorist attacks and other high-consequence events utilizing chemical agents, such as at ports, areas of mass gathering, and transit facilities, and may—

“(1) ensure all high-risk situations and venues are studied; and

“(2) ensure key findings and best practices are made available to State, local, tribal, and territorial governments and the private sector.

“(c) CONGRESSIONAL NOTIFICATION.—The Director shall notify the Committee on Homeland Security of the House of Representatives and the Committee on Homeland Security and Governmental Affairs of the Senate not later than 30 days before initiating a new demonstration project.”.

(b) REPORT.—Not later than 1 year after the date of the enactment of this Act, the Comptroller General of the United States shall submit to the Committee on Homeland Security of the House of Representatives and the Committee on Homeland Security and Governmental Affairs of the Senate an assessment of the Department of Homeland Security’s programs and activities related to terrorist attacks and other high-consequence events utilizing chemical agents that pose a high risk to homeland security.
SEC. 903. BIOLOGICAL DIVISION.

Title XXII of the Homeland Security Act of 2002, as added by section 901 of this title and as amended by section 902 of this title, is further amended by adding at the end the following new subtitle:

“Subtitle C—Biological Division

“SEC. 2221. BIOLOGICAL DIVISION.

“(a) Establishment.—There is established in the CBRNE Office a Biological Division, headed by a Director of the Biological Division (in this subtitle referred to as the ‘Director’).

“(b) Mission and Responsibilities.—The Office shall be responsible for coordinating departmental strategy and policy relating to terrorist attacks and other high-consequence events utilizing biological agents that pose a high risk to homeland security, including the following:

“(1) Developing and maintaining the Department’s strategy against biological threats.

“(2) Serving as the Department representative for biological threats and related activities with other Federal departments and agencies.

“(3) Providing oversight for the Department’s preparedness, including operational requirements, for biological threats.

“(4) Enhancing the capabilities of Federal, State, local, tribal, and territorial governments, and
private entities as appropriate, against biological threats.

“(5) Supporting and enhancing the effective sharing and use of appropriate information generated by the intelligence community (as such term is defined in section 3(4) of the National Security Act of 1947 (50 U.S.C. 3003(4))), law enforcement agencies, other Federal, State, local, tribal, and territorial governments, and foreign governments, on biological threats.

“(6) Achieving a biological detection program.

“(7) Maintaining the National Biosurveillance Integration Center, authorized under section 316.”.

SEC. 904. NUCLEAR DIVISION.

(a) IN GENERAL.—Title XXII of the Homeland Security Act of 2002, as added by section 901 of this title and as amended by sections 902 and 903 of this title, is further amended by adding at the end the following new subtitle:

“Subtitle D—Nuclear Division

“SEC. 2231. NUCLEAR DIVISION.

“(a) ESTABLISHMENT.—The Secretary shall include within the CBRNE Office the Nuclear Division under title XIX, headed by the Director of the Nuclear Division (in
this subtitle referred to as the ‘Director’) pursuant to sec-
tion 1901.

“(b) MISSION AND RESPONSIBILITIES.—In addition to the responsibilities specified in title XIX, the Director shall also be responsible for coordinating departmental strategy and policy relating to terrorist attacks and other high-consequence events utilizing nuclear or other radiological materials, and for coordinating Federal efforts to detect and protect against the unauthorized importation, possession, storage, transportation, development, or use of a nuclear explosive device, fissile material, or radiological material in the United States, and to protect against an attack using such devices or materials against the people, territory, or interests of the United States, in accordance with title XIX.”.

(b) TECHNICAL AND CONFORMING AMENDMENTS.—Title XIX of the Homeland Security Act of 2002 is amended—

(1) in the title heading, by striking “DOMES-
TIC NUCLEAR DETECTION OFFICE” and inserting “NUCLEAR DIVISION”;

(2) in section 1901 (6 U.S.C. 591)—

(A) in the heading, by striking “DOMES-
TIC NUCLEAR DETECTION OFFICE” and in-
serting “NUCLEAR DIVISION”;
(B) in subsection (a), by striking “There shall be established in the Department a Domestic Nuclear Detection Office” and inserting “There is in the Department a Nuclear Division, located in the CBRNE Office”; and

(C) in subsection (b), by striking “Director for Domestic Nuclear Detection, who shall be appointed by the President” and inserting “Director of the Nuclear Division”;

(3) in subsection (a) of section 1902 (6 U.S.C. 592)—

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

(i) by inserting after “responsible for” the following: “coordinating departmental strategy and policy relating to terrorist attacks and other high-consequence events utilizing nuclear or other radiological materials, and for”; and

(ii) by striking “to protect” and inserting “protecting”; and

(B) in paragraph (11), in the matter preceding subparagraph (A), by striking “Domestic Nuclear Detection Office” and inserting “Nuclear Division”;

•HR 6381 IH
(4) by repealing section 1903 (6 U.S.C. 593);

(5) in section 1906 (6 U.S.C. 596)—

(A) in the matter preceding paragraph

(1)—

(i) by striking “Domestic Nuclear De-
tection” and inserting “the Nuclear Divi-
sion”; and

(ii) by striking “paragraphs (6) and
(7) of”; and

(B) in paragraph (2), by striking “para-
graphs (6) and (7) of”;

(6) in section 1907 (6 U.S.C. 596a)—

(A) by striking “Annual” each place it ap-
pears and inserting “Biennial”;

(B) by striking “each year” each place it
appears and inserting “every 2 years”;

(C) by striking “previous year” each place
it appears and inserting “previous 2 years”;

(D) in the heading of subsection (a), by
striking “ANNUAL” and inserting “BIENNIAL”;

and

(E) subsection (b)—

(i) in the heading, by striking “AN-
NUAL” and inserting “BIENNIAL”;
(ii) in paragraph (1), by inserting “odd-numbered” after “each”; and

(iii) in paragraph (2), by striking “annual” and inserting “biennial”; and

(7) by adding at the end the following new section:

“SEC. 1908. DOMESTIC IMPLEMENTATION OF THE GLOBAL NUCLEAR DETECTION ARCHITECTURE.

“In carrying out the mission of the Office under subparagraph (A) of section 1902(a)(4), the Director of the Nuclear Division shall provide support for planning, organization, equipment, training, exercises, and operational assessments to Federal, State, local, tribal, and territorial governments to assist such governments in implementing radiological and nuclear detection capabilities in the event of terrorist attacks or other high-consequence events utilizing nuclear or other radiological materials that pose a high risk to homeland security. Such capabilities shall be integrated into the enhanced global nuclear detection architecture referred to in such section 1902(a)(4), and shall inform and be guided by architecture studies, technology needs, and research activities of the Office.”.

(e) REFERENCE.—Any reference in any law, regulation, or rule to the Domestic Nuclear Detection Office or the Director for Domestic Nuclear Detection of the De-
part of Homeland Security shall be deemed to be a reference to the Nuclear Division or the Director of the Nuclear Division, respectively, of the Department.

SEC. 905. EXPLOSIVES DIVISION.

Title XXII of the Homeland Security Act of 2002, as added by section 1001 of this title and as amended by sections 1002, 1003, and 1004 of this title, is further amended by adding at the end the following new subtitle:

“Subtitle E—Explosives Division

“SEC. 2241. EXPLOSIVES DIVISION.

“(a) Establishment.—There is established within the CBRNE Office an Explosives Division, headed by a Director of the Explosives Division (in this subtitle referred to as the ‘Director’).

“(b) Mission and Responsibilities.—The Director shall be responsible for coordinating departmental strategy and policy relating to terrorist attacks and other high-consequence events utilizing explosives that pose a high risk to homeland security, including the following:

“(1) Developing and maintaining the Department’s strategy against explosives threats.

“(2) Serving as the Department representative for explosives threats and related activities with other Federal departments and agencies.
“(3) Providing oversight of the Department’s preparedness, including operational requirements, for explosives threats.

“(4) Enhancing the capabilities of Federal, State, local, tribal, and territorial governments, and private entities as appropriate, to counter terrorist attacks and other high-consequence events utilizing explosives.

“(5) Evaluating and providing guidance to Federal, State, local, tribal, and territorial governments and appropriate private entities on detection and communication technology that could be effective during terrorist attacks or other high-consequence events utilizing explosives.

“(6) Supporting and enhancing the effective sharing and use of appropriate information generated by the intelligence community (as such term is defined in section 3(4) of the National Security Act of 1947 (50 U.S.C. 3003(4))), law enforcement agencies, other Federal, State, local, tribal, and territorial government agencies, and foreign governments, on explosives threats.”.

SEC. 906. SAVINGS PROVISIONS.

Nothing in this title shall change the authority of the Administrator of the Federal Emergency Management
Agency to lead the emergency management system of the United States. Nothing in this title shall alter the responsibility of the Chief Medical Officer of the Department of Homeland Security to serve as the principal advisor to the Secretary of Homeland Security and the Administrator of the Federal Emergency Management Agency on medical and public health issues pursuant to paragraph (1) of section 516(e) of the Homeland Security Act of 2002 (6 U.S.C. 321e(e)).

SEC. 907. CLERICAL AMENDMENTS.

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

(1) by striking the item relating to title XIX and inserting the following new item:

“TITLE XIX—NUCLEAR DIVISION”;

(2) by striking the item relating to section 1901 and inserting the following new item:

“Sec. 1901. Nuclear Division.”;

(3) by striking the item relating to section 1903;

(4) by adding after the item relating to section 1907 the following new item:

“Sec. 1908. Domestic Implementation of the global nuclear detection architecture.”;

and

(5) by adding at the end the following:

“TITLE XXII—CBRNE OFFICE
“Subtitle A—Chemical, Biological, Radiological, Nuclear, and Explosives Office

“Sec. 2201. Chemical, Biological, Radiological, Nuclear, and Explosives Office.
“Sec. 2202. Composition of the CBRNE Office.
“Sec. 2203. Hiring authority.
“Sec. 2204. Grants, cooperative agreements, and other transactions and contracts.
“Sec. 2205. Terrorism risk assessments.
“Sec. 2206. CBRNE communications and public messaging.
“Sec. 2207. Chemical, biological, radiological, nuclear, and explosives intelligence and information sharing.

“Subtitle B—Chemical Division

“Sec. 2211. Chemical Division.
“Sec. 2212. Demonstration projects.

“Subtitle C—Biological Division

“Sec. 2221. Biological Division.

“Subtitle D—Nuclear Division

“Sec. 2231. Nuclear Division.

“Subtitle E—Explosives Division

“Sec. 2241. Explosives Division.”.

1 TITLE X—GAINS IN GLOBAL NUCLEAR DETECTION ARCHITECTURE

2 SEC. 1001. DUTIES OF THE DOMESTIC NUCLEAR DETECTION OFFICE.

3 Section 1902 of the Homeland Security Act of 2002 (6 U.S.C. 592) is amended—

4 (1) by redesignating subsection (b) as subsection (c); and

5 (2) by inserting after subsection (a) the following new subsection:
'(b) IMPLEMENTATION.—In carrying out paragraph (6) of subsection (a), the Director of the Domestic Nuclear Detection Office shall—

‘‘(1) develop and maintain documentation, such as a technology roadmap and strategy, that—

‘‘(A) provides information on how the Office’s research investments align with—

‘‘(i) gaps in the enhanced global nuclear detection architecture, as developed pursuant to paragraph (4) of such subsection; and

‘‘(ii) research challenges identified by the Director; and

‘‘(B) defines in detail how the Office will address such research challenges;

‘‘(2) document the rational for prioritizing and selecting research topics; and

‘‘(3) develop a systematic approach, which may include annual metrics and periodic qualitative evaluations, for evaluating how the outcomes of the Office’s individual research projects collectively contribute to addressing the Office’s research challenges.’’.
TITLE XI—UNITED STATES IMMIGRATION AND CUSTOMS ENFORCEMENT AUTHORIZATION

SEC. 1101. ESTABLISHMENT OF UNITED STATES IMMIGRATION AND CUSTOMS ENFORCEMENT.

(a) In General.—Section 442 of the Homeland Security Act of 2002 (6 U.S.C. 252) is amended to read as follows:

“SEC. 442. ESTABLISHMENT OF UNITED STATES IMMIGRATION AND CUSTOMS ENFORCEMENT.

“(a) Establishment.—There is established within the Department an agency to be known as United States Immigration and Customs Enforcement.

“(b) Director of United States Immigration and Customs Enforcement.—There shall be at the head of United States Immigration and Customs Enforcement a Director of United States Immigration and Customs Enforcement (in this section referred to as the ‘Director’).

“(c) Duties and Qualifications.—The Director shall—

“(1) have a minimum of five years professional experience in law enforcement, which may include law enforcement as it relates to the immigration or customs laws, as defined by titles 8, 18, 19, and 31,
United States Code, and a minimum of five years management experience;

“(2) enforce the immigration laws, as defined in title 8, United States Code, and seek the removal of aliens identified as inadmissible and deportable;

“(3) have the power to investigate and, where appropriate, refer for prosecution, any criminal violation of Federal law relating to or involving—

“(A) border control and security, including the prevention of the entry or residence of terrorists, criminals, and human rights violators;

“(B) customs, trade, fraud, false statements, or the import or export of merchandise, including the illicit possession, movement of, or trade in goods, services, property, arms, instruments of terrorism, items controlled or prohibited from export, child exploitation, intellectual property, or monetary instruments;

“(C) cross-border money laundering or bulk cash smuggling;

“(D) the immigration laws, as defined in section 101(a)(17) of the Immigration and Nationality Act;

“(E) gangs or criminal syndicates engaged in cross-border criminal activity;
“(F) chapter 40 or 44 of title 18, United States Code, or other violation relating to firearms, explosives, or other destructive devices involving an alien;

“(G) trafficking in persons, as defined in section 7102 of title 22, United States Code;

“(H) the production, procurement, counterfeiting, alteration or use of fraudulent immigration documents or fraudulently obtaining immigration benefits;

“(I) unlawful use of personal information, when such use relates to or affects border security, terrorism, customs, immigration, naturalization, trade, or transportation security; and

“(J) computer crimes, pursuant to section 1030(d) of title 18 United States Code, in collaboration with the United States Secret Service and the Federal Bureau of Investigation;

“(4) coordinate, as otherwise permitted by law, with Federal, State, local, tribal, and foreign agencies in carrying out the duties set forth in paragraphs (2) and (3);

“(5) in coordination with the Department of State and the Office of International Affairs of the Department, establish staff liaison offices and vetted
units in foreign countries to support law enforce-
ment activities that require international coopera-
tion, including investigations and repatriation ef-
forts;

“(6) establish, maintain, and administer appro-
priate interagency law enforcement centers in fur-
therance of the Director’s assigned duties, including
the Centers specified in subparagraphs (B) and (C)
of subsection (f)(3); and

“(7) carry out the duties and powers prescribed
by law or delegated by the Secretary.

“(d) GENERAL ENFORCEMENT POWERS.—The Di-
rector may authorize agents and officers of United States
Immigration and Customs Enforcement to—

“(1) carry out the duties and responsibilities
authorized under section 1357 of title 8, United
States Code, and section 1589a of title 19, United
States Code;

“(2) seize any property, whether real or per-
sonal, that is involved in any violation or attempted
violation, or which constitutes proceeds traceable to
a violation, of those provisions of law which United
States Immigration and Customs Enforcement is au-
thorized to enforce;
“(3) offer and pay rewards for services and information regarding the apprehension of persons involved in, or the seizure and forfeiture of property associated with, the violation or attempted violation of those provisions of law which United States Immigration and Customs Enforcement is authorized to enforce;

“(4) issue civil detainers for purposes of immigration enforcement; and

“(5) conduct undercover investigative operations pursuant to section 1363a of title 8, United States Code, and section 2081 of title 19, United States Code.

“(e) DEPUTY DIRECTOR.—There shall be in United States Immigration and Customs Enforcement a Deputy Director who shall assist the Director in the management of United States Immigration and Customs Enforcement.

“(f) OFFICE OF HOMELAND SECURITY INVESTIGATIONS.—

“(1) IN GENERAL.—There is established in United States Immigration and Customs Enforcement the Office of Homeland Security Investigations.

“(2) EXECUTIVE ASSOCIATE DIRECTOR.—There shall be at the head of the Office of Homeland Secu-
The Office of Homeland Security Investigations shall—

“(A) serve as the law enforcement office of United States Immigration and Customs Enforcement with primary responsibility to conduct investigations of terrorist organizations and other criminal organizations that threaten homeland or border security;

“(B) serve as the law enforcement office of U.S. Immigration and Customs Enforcement with primary responsibility to conduct investigations of criminal violations of the immigration and customs laws, as defined in titles 8, 18, and 19, United States Code;

“(C) identify, arrest, detain, bring removal proceedings against and pursue the removal of aliens who are inadmissible or deportable;

“(D) administer the program to collect information relating to nonimmigrant foreign students and other exchange program participants described in section 641 of the Illegal Immigration Reform and Immigrant Responsibility Act of 1996 (8 U.S.C. 1372), including the Student
and Exchange Visitor Information System est-
ablished under such section, and use such in-
formation to carry out the enforcement func-
tions of United States Immigration and Cus-
toms Enforcement;

“(E) administer a National Intellectual
Property Rights Coordination Center, which
shall serve as the primary forum within the
Federal Government to coordinate, promote,
and assist Federal and international investiga-
tions of intellectual property offenses;

“(F) administer a National Export En-
f orcement Coordination Center, which shall
serve as the primary forum within the Federal
Government to coordinate, promote, and assist
Federal and international investigations of Ex-
port Control offenses;

“(G) enforce Federal law relating to—

“(i) the unlawful employment of un-
authorized aliens, as defined in section
274A(h)(3) of the Immigration and Na-
tionality Act; and

“(ii) immigration and naturalization
fraud;
“(H) administer the Cyber Crimes Center, as authorized under section 890A of the Homeland Security Act of 2002 (6 U.S.C. 473); and
“(I) carry out other duties and powers prescribed by the Director.

“(g) Office of Enforcement and Removal Operations.—

“(1) In general.—There is established in United States Immigration and Customs Enforcement the Office of Enforcement and Removal Operations.

“(2) Executive Associate Director.—There shall be at the head of the Office of Enforcement and Removal Operations an Executive Associate Director, who shall report to the Director.

“(3) Duties.—The Office of Enforcement and Removal Operations shall—

“(A) serve as the law enforcement office of U.S. Immigration and Customs Enforcement with primary responsibility to enforce the civil immigration and nationality laws of the United States;

“(B) identify, locate, and arrest aliens in custodial settings or at-large two are subject to
exclusion, deportation, or removal from the United States;

“(C) manage the ICE administrative detention operations and provide medical care, dental, and mental health services to detained aliens in the custody of the agency;

“(D) detain or release on bond, supervision, or other appropriate condition, aliens for purposes of exclusion, deportation, or removal from the United States;

“(E) plan, coordinate, and manage the removal from the United States of aliens who are subject to exclusion, deportation, or removal from the United States;

“(F) provide law enforcement support services to Federal, State, and local law enforcement partner agencies, relating to the identification, location, and arrest of aliens subject to removal from the United States, as well as foreign-nationals known or suspected to be involved in criminal activity and under investigation by these partners; and

“(G) carry out other duties and powers prescribed by the Director.

“(h) OFFICE OF THE PRINCIPAL LEGAL ADVISOR.—
“(1) In general.—There is established in
United States Immigration and Customs Enforce-
ment the Office of the Principal Legal Advisor.

“(2) Principal Legal Advisor.—There shall
be at the head of the Office the Principal Legal Ad-
visor a Principal Legal Advisor, who, for legal mat-
ters, shall report to the General Counsel of the De-
partment.

“(3) Duties.—The Office of the Principal
Legal Advisor shall—

“(A) provide specialized legal advice and
policy guidance to the Director;

“(B) represent the Department in all ex-
clusion, deportation, and removal proceedings
before the Executive Office for Immigration Re-
view;

“(C) represent the United States Immigra-
tion and Customs Enforcement in matters be-
fore the Office of the Chief Administrative
Hearing Officer; and

“(D) represent the United States Immigra-
tion and Customs Enforcement in other venues
and forums as authorized by the Director.

“(i) Office of Professional Responsibility.—
“(1) IN GENERAL.—There is established in the United States Immigration and Customs Enforcement the Office of Professional Responsibility.

“(2) ASSISTANT DIRECTOR.—There shall be at the head of the Office of Professional Responsibility an Assistant Director, who shall report to the Director.

“(3) DUTIES.—The Office of Professional Responsibility shall—

“(A) investigate allegations of administrative, civil, and criminal misconduct involving any employee or contractor of United States Immigration and Customs Enforcement, or, as delegated by the Secretary, any employee or contractor of the Department;

“(B) inspect and review United States Immigration and Customs Enforcement’s offices, operations, and processes, including detention facilities operated or used by United States Immigration and Customs Enforcement, and provide an independent review of United States Immigration and Custom Enforcement’s organizational health, effectiveness, and efficiency of mission; and
“(C) provide and manage the security programs and operations for United States Immigration and Customs Enforcement.

“(j) Office of Policy.—

“(1) In general.—There is established in United States Immigration and Customs Enforcement the Office of Policy.

“(2) Duties.—The Office of the Policy shall—

“(A) identify and develop policies and guidance of U.S. Immigration and Customs Enforcement;

“(B) provide policy recommendations, research and analysis to the Director; and

“(C) coordinate policy issues with the Department, components of the Department, and other federal, state, and local agencies and offices.

“(k) Other Authorities.—

“(1) In general.—The Secretary may establish such other Executive Associate Directors, Assistant Directors, agents, officers, or other offices as the Secretary determines necessary to carry out the missions, duties, functions, and authorities of United States Immigration and Customs Enforcement.
“(2) NOTIFICATION.—If the Secretary exercises the authority provided pursuant to paragraph (1), the Secretary shall notify the Committee on Homeland Security and the Committee on the Judiciary of the House of Representatives and the Committee on Homeland Security and Governmental Affairs and the Committee on the Judiciary of the Senate not later than 30 days before exercising the authority described in paragraph (1).

“(l) OTHER FEDERAL AGENCIES.—Nothing in this section shall be construed to limit the existing authority of any other Federal agency.”.

(b) SPECIAL RULES.—

(1) TREATMENT.—Section 442 of the Homeland Security Act of 2002, as amended by subsection (a) of this section, shall be treated as if included in such Act as of the date of the enactment of such Act, and, in addition to the functions, missions, duties, and authorities specified in such amended section 442, United States Immigration and Customs Enforcement shall continue to perform and carry out the functions, missions, duties, and authorities under section 442 of such Act as in existence on the day before such date of enactment.

(2) RULES OF CONSTRUCTION.—
(A) Rules and Regulations.—Notwithstanding paragraph (1), nothing in this title may be construed as affecting in any manner any rule or regulation issued or promulgated pursuant to any provision of law, including section 442 of the Homeland Security Act of 2002 as in existence on the day before the date of the enactment of this Act, and any such rule or regulation shall continue to have full force and effect on and after such date.

(B) Other Actions.—Notwithstanding paragraph (1), nothing in this title may be construed as affecting in any manner any action, determination, policy, or decision pursuant to section 442 of the Homeland Security Act of 2002 as in existence on the day before the date of the enactment of this Act, and any such action, determination, policy, or decision shall continue to have full force and effect on and after such date.

c) Continuation in Office.—

(1) Director.—The individual serving as Assistant Secretary for United States Immigration and Customs Enforcement on the day before the date of the enactment of this Act may continue to serve as
the Director of United States Immigration and Customs Enforcement in accordance with section 442 of the Homeland Security Act of 2002, as amended by this title until the earlier of—

(A) the date on which such individual is no longer eligible to serve as Director; or

(B) the date on which a person nominated by the President to be the Director is confirmed by the Senate in accordance with such amended section 442.

(2) Other positions.—The individuals serving as the Deputy Director, Executive Associate Directors, Deputy Executive Associate Directors, Assistant Directors, and other officers and employees under section 442 of the Homeland Security Act of 2002 on the day before the date of the enactment of this Act may serve as the appropriate Deputy Director, Executive Associate Directors, Deputy Executive Associate Directors, Assistant Directors, and other officers and employees under such section 442 as amended by subsection (a) of this section unless the Director of United States Immigration and Customs Enforcement determines that another individual should hold such position.
(d) **CLERICAL AMENDMENT.**—The table of contents in section 1(b) of such Act is amended by striking the item relating to section 442 and inserting the following:

"Sec. 442. Establishment of United States Immigration and Customs Enforcement."

(e) **TRANSPORTATION.**—Section 1344(b)(6) of title 31, United States Code, is amended by inserting "‘the Director of United States Immigration and Customs Enforcement, the Commissioner of Customs and Border Protection,’" after "‘the Administrator of the Drug Enforcement Administration,’".

(f) **CONFORMING AMENDMENTS.**—

(1) **TITLE 5.**—Section 5314 of title 5, United States Code, is amended by inserting after "Director of the Bureau of Citizenship and Immigration Services." the following new item: "Director of United States Immigration and Customs Enforcement."

(2) **HOMELAND SECURITY ACT OF 2002.**—The Homeland Security Act of 2002 is amended—

(A) in subsection (a)(2)(C) of section 451 (6 U.S.C. 271), by striking "‘at the same level as the Assistant Secretary of the Bureau of Border Security’" and inserting "‘in accordance with section 5314 of title 5, United States Code’";
(B) in subsection (c) of section 459 (6 U.S.C. 276), by striking “Assistant Secretary of the Bureau of Border Security” and inserting “Director of United States Immigration and Customs Enforcement”;

(C) in subsection (b)(2)(A) of section 462 (6 U.S.C. 279), in the matter preceding clause (i), by striking “Assistant Secretary of the Bureau of Border Security” and inserting “Director of United States Immigration and Customs Enforcement”;

(D) by repealing sections, 445, and 446 (6 U.S.C. 255, and 256); and

(E) in section 1(b), by striking the items relating to sections 445 and 446.

(3) Title 8.—Section 1357 of title 8, United States Code is amended in section (a)(5)(B) by striking “if the officer or employee is performing duties relating to the enforcement of the immigration laws at the time of the arrest and if there is a likelihood of the person escaping before a warrant can be obtained for his arrest”.

•HR 6381 IH
TITLE XII—FEDERAL LAW ENFORCEMENT TRAINING CENTERS REFORM AND IMPROVEMENT

SEC. 1201. FEDERAL LAW ENFORCEMENT TRAINING CENTERS.

(a) ESTABLISHMENT.—Section 884 of the Homeland Security Act of 2002 (6 U.S.C. 464) is amended to read as follows:

“SEC. 884. FEDERAL LAW ENFORCEMENT TRAINING CENTERS.

“(a) ESTABLISHMENT.—The Secretary shall maintain in the Department the Federal Law Enforcement Training Centers (FLETC), headed by a Director, who shall report to the Secretary.

“(b) POSITION.—The Director shall occupy a career-reserved position within the Senior Executive Service.

“(c) FUNCTIONS OF THE DIRECTOR.—The Director shall—

“(1) develop training goals and establish strategic and tactical organizational program plan and priorities;

“(2) provide direction and management for FLETC’s training facilities, programs, and support activities while ensuring that organizational program
goals and priorities are executed in an effective and
efficient manner;

“(3) develop homeland security and law en-
forcement training curricula, including curricula re-
lated to domestic preparedness and response to
threats or acts of terrorism, for Federal, State, local,
tribal, territorial, and international law enforcement
and security agencies and private sector security
agencies;

“(4) monitor progress toward strategic and tac-
tical FLETC plans regarding training curricula, in-
cluding curricula related to domestic preparedness
and response to threats or acts of terrorism, and fa-
cilities;

“(5) ensure the timely dissemination of home-
land security information as necessary to Federal,
State, local, tribal, territorial, and international law
enforcement and security agencies and the private
sector to achieve the training goals for such entities,
in accordance with paragraph (1);

“(6) carry out acquisition responsibilities in a
manner that—

“(A) fully complies with—

“(i) Federal law;
“(ii) the Federal Acquisition Regulation, including requirements regarding agency obligations to contract only with responsible prospective contractors; and

“(iii) Department acquisition management directives; and

“(B) ensures that a fair proportion of Federal contract and subcontract dollars are awarded to small businesses, maximizes opportunities for small business participation, and ensures, to the extent practicable, that small businesses which achieve qualified vendor status for security-related technologies have an opportunity to compete for contracts for such technologies;

“(7) coordinate and share information with the heads of relevant components and offices on digital learning and training resources, as appropriate;

“(8) advise the Secretary on matters relating to executive level policy and program administration of Federal, State, local, tribal, territorial, and international law enforcement and security training activities and private sector security agency training activities, including training activities related to domestic preparedness and response to threats or acts of terrorism;
“(9) collaborate with the Secretary and relevant officials at other Federal departments and agencies, as appropriate, to improve international instructional development, training, and technical assistance provided by the Federal Government to foreign law enforcement; and

“(10) carry out such other functions as the Secretary determines are appropriate.

“(d) TRAINING RESPONSIBILITIES.—

“(1) IN GENERAL.—The Director is authorized to provide training to employees of Federal agencies who are engaged, directly or indirectly, in homeland security operations or Federal law enforcement activities, including such operations or activities related to domestic preparedness and response to threats or acts of terrorism. In carrying out such training, the Director shall—

“(A) evaluate best practices of law enforcement training methods and curriculum content to maintain state-of-the-art expertise in adult learning methodology;

“(B) provide expertise and technical assistance, including on domestic preparedness and response to threats or acts of terrorism, to Federal, State, local, tribal, territorial, and inter-
national law enforcement and security agencies
and private sector security agencies; and

“(C) maintain a performance evaluation
process for students.

“(2) RELATIONSHIP WITH LAW ENFORCEMENT
AGENCIES.—The Director shall consult with relevant
law enforcement and security agencies in the devel-
opment and delivery of FLETC’s training programs.

“(3) TRAINING DELIVERY LOCATIONS.—The
training required under paragraph (1) may be con-
ducted at FLETC facilities, at appropriate off-site
locations, or by distributed learning.

“(4) STRATEGIC PARTNERSHIPS.—

“(A) IN GENERAL.—The Director may—

“(i) execute strategic partnerships
with State and local law enforcement to
provide such law enforcement with specific
training, including maritime law enforce-
ment training; and

“(ii) coordinate with the Under Sec-
retary responsible for overseeing critical in-
frastructure protection, cybersecurity, and
other related programs of the Department
and with private sector stakeholders, in-
cluding critical infrastructure owners and
operators, to provide training pertinent to improving coordination, security, and resiliency of critical infrastructure.

“(B) PROVISION OF INFORMATION.—The Director shall provide to the Committee on Homeland Security of the House of Representatives and the Committee on Homeland Security and Governmental Affairs of the Senate, upon request, information on activities undertaken in the previous year pursuant to subparagraph (A).

“(5) FLETC DETAILS TO DHS.—The Director may detail employees of FLETC to positions throughout the Department in furtherance of improving the effectiveness and quality of training provided by the Department and, as appropriate, the development of critical departmental programs and initiatives.

“(6) DETAIL OF INSTRUCTORS TO FLETC.—Partner organizations that wish to participate in FLETC training programs shall assign non-reimbursable detailed instructors to FLETC for designated time periods to support all training programs at FLETC, as appropriate. The Director shall determine the number of detailed instructors
that is proportional to the number of training hours requested by each partner organization scheduled by FLETC for each fiscal year. If a partner organization is unable to provide a proportional number of detailed instructors, such partner organization shall reimburse FLETC for the salary equivalent for such detailed instructors, as appropriate.

“(7) Partner Organization Expenses Requirements.—

“(A) In General.—Partner organizations shall be responsible for the following expenses:

“(i) Salaries, travel expenses, lodging expenses, and miscellaneous per diem allowances of their personnel attending training courses at FLETC.

“(ii) Salaries and travel expenses of instructors and support personnel involved in conducting advanced training at FLETC for partner organization personnel and the cost of expendable supplies and special equipment for such training, unless such supplies and equipment are common to FLETC-conducted training and have been included in FLETC’s budget for the applicable fiscal year.
“(B) Excess basic and advanced federal training.—All hours of advanced training and hours of basic training provided in excess of the training for which appropriations were made available shall be paid by the partner organizations and provided to FLETC on a reimbursable basis in accordance with section 4104 of title 5, United States Code.

“(8) Provision of non-federal training.—

“(A) In general.—The Director is authorized to charge and retain fees that would pay for its actual costs of the training for the following:

“(i) State, local, tribal, and territorial law enforcement personnel.

“(ii) Foreign law enforcement officials, including provision of such training at the International Law Enforcement Academies wherever established.

“(iii) Private sector security officers, participants in the Federal Flight Deck Officer program under section 44921 of title 49, United States Code, and other appropriate private sector individuals.
“(B) WAIVER.—The Director may waive
the requirement for reimbursement of any cost
under this section and shall maintain records
regarding the reasons for any requirements so
waived.

“(9) REIMBURSEMENT.—The Director is au-
thorized to reimburse travel or other expenses for
non-Federal personnel who attend activities related
to training sponsored by FLETC, at travel and per
diem rates established by the General Services Ad-
ministration.

“(10) STUDENT SUPPORT.—In furtherance of
its training mission, the Director is authorized to
provide the following support to students:

“(A) Athletic and related activities.

“(B) Short-term medical services.

“(C) Chaplain services.

“(11) AUTHORITY TO HIRE FEDERAL ANNU-
ITANTS.—

“(A) IN GENERAL.—Notwithstanding any
other provision of law, the Director is author-
ized to appoint and maintain, as necessary,
Federal annuitants who have expert knowledge
and experience to meet the training responsibil-
ities under this subsection.
“(B) No reduction in retirement pay.—A Federal annuitant employed pursuant to this paragraph shall not be subject to any reduction in pay for annuity allocable to the period of actual employment under the provisions of section 8344 or 8468 of title 5, United States Code, or similar provision of any other retirement system for employees.

“(C) Re-employed annuitants.—A Federal annuitant employed pursuant to this paragraph shall not be considered an employee for purposes of subchapter III of chapter 83 or chapter 84 of title 5, United States Code, or such other retirement system (referred to in subparagraph (B)) as may apply.

“(D) Counting.—Federal annuitants shall be counted on a full time equivalent basis.

“(E) Limitation.—No appointment under this paragraph may be made which would result in the displacement of any employee.

“(12) Travel for intermittent employees.—The Director is authorized to reimburse intermittent Federal employees traveling from outside a commuting distance (to be predetermined by the Director) for travel expenses and to compensate such
employees for time spent traveling from their homes to work sites.

“(e) ON-FLETC HOUSING.—Notwithstanding any other provision of law, individuals attending training at any FLETC facility shall, to the extent practicable and in accordance with FLETC policy, reside in on-FLETC or FLETC-provided housing.

“(f) ADDITIONAL FISCAL AUTHORITIES.—In order to further the goals and objectives of FLETC, the Director is authorized to—

“(1) expend funds for public awareness and to enhance community support of law enforcement training, including the advertisement of available law enforcement training programs;

“(2) accept and use gifts of property, both real and personal, and to accept gifts of services, for purposes that promote the functions of the Director pursuant to subsection (c) and the training responsibilities of the Director under subsection (d);

“(3) accept reimbursement from other Federal agencies for the construction or renovation of training and support facilities and the use of equipment and technology on government owned-property;

“(4) obligate funds in anticipation of reimbursements from agencies receiving training at
FLETC, except that total obligations at the end of a fiscal year may not exceed total budgetary resources available at the end of such fiscal year;

“(5) in accordance with the purchasing authority provided under section 505 of the Department of Homeland Security Appropriations Act, 2004 (Public Law 108–90; 6 U.S.C. 453a)—

“(A) purchase employee and student uniforms; and

“(B) purchase and lease passenger motor vehicles, including vehicles for police-type use;

“(6) provide room and board for student interns; and

“(7) expend funds each fiscal year to honor and memorialize FLETC graduates who have died in the line of duty.

“(g) DEFINITIONS.—In this section:

“(1) BASIC TRAINING.—The term ‘basic training’ means the entry-level training required to instill in new Federal law enforcement personnel fundamental knowledge of criminal laws, law enforcement and investigative techniques, laws and rules of evidence, rules of criminal procedure, constitutional rights, search and seizure, and related issues.
“(2) Detailed Instructors.—The term ‘detailed instructors’ means personnel who are assigned to the Federal Law Enforcement Training Centers for a period of time to serve as instructors for the purpose of conducting basic and advanced training.

“(3) Director.—The term ‘Director’ means the Director of the Federal Law Enforcement Training Centers.

“(4) Distributed Learning.—The term ‘distributed learning’ means education in which students take academic courses by accessing information and communicating with the instructor, from various locations, on an individual basis, over a computer network or via other technologies.

“(5) Employee.—The term ‘employee’ has the meaning given such term in section 2105 of title 5, United States Code.

“(6) Federal Agency.—The term ‘Federal agency’ means—

“(A) an Executive Department as defined in section 101 of title 5, United States Code;

“(B) an independent establishment as defined in section 104 of title 5, United States Code;
“(C) a Government corporation as defined in section 9101 of title 31, United States Code;
“(D) the Government Publishing Office;
“(E) the United States Capitol Police;
“(F) the United States Supreme Court Police; and
“(G) Government agencies with law enforcement related duties.
“(7) LAW ENFORCEMENT PERSONNEL.—The term ‘law enforcement personnel’ means an individual, including criminal investigators (commonly known as ‘agents’) and uniformed police (commonly known as ‘officers’), who has statutory authority to search, seize, make arrests, or to carry firearms.
“(8) LOCAL.—The term ‘local’ means—
“(A) of or pertaining to any county, parish, municipality, city, town, township, rural community, unincorporated town or village, local public authority, educational institution, special district, intrastate district, council of governments (regardless of whether the council of governments is incorporated as a nonprofit corporation under State law), regional or inter-state government entity, any agency or instru-
mentality of a local government, or any other political subdivision of a State; and

“(B) an Indian tribe or authorized tribal organization, or in Alaska a Native village or Alaska Regional Native Corporation.

“(9) PARTNER ORGANIZATION.—The term ‘partner organization’ means any Federal agency participating in FLETC’s training programs under a formal memorandum of understanding.

“(10) STATE.—The term ‘State’ means any State of the United States, the District of Columbia, the Commonwealth of Puerto Rico, the Virgin Islands, Guam, American Samoa, the Commonwealth of the Northern Mariana Islands, and any possession of the United States.

“(11) STUDENT INTERN.—The term ‘student intern’ means any eligible baccalaureate or graduate degree student participating in FLETC’s College Intern Program.

“(h) PROHIBITION ON NEW FUNDING.—No funds are authorized to carry out this section. This section shall be carried out using amounts otherwise appropriated or made available for such purpose.”.

(b) CLERICAL AMENDMENT.—The table of contents in section 1(b) of the Homeland Security Act of 2002 is
amended by amending the item relating to section 884 to read as follows:

“Sec. 884. Federal Law Enforcement Training Centers.”.

TITLE XIII—PREVENT TRAFFICKING IN CULTURAL PROPERTY

SEC. 1301. DEFINITION.

In this title, the term “cultural property” includes property covered under—


SEC. 1302. STATEMENT OF POLICY.

It shall be the policy of the United States to—

(1) ensure the components of the Department of Homeland Security enhance and unify efforts to—
(A) interdict, detain, seize, and investigate cultural property illegally imported into the United States;

(B) disrupt and dismantle smuggling and trafficking networks and transnational criminal organizations engaged in, conspiring to engage in, or facilitating illegal trade in cultural property, including stolen antiquities used to finance terrorism; and

(C) support Offices of United States Attorneys in prosecuting persons engaged in, conspiring to engage in, or facilitating illegal trade in cultural property; and

SEC. 1303. ACTIVITIES OF THE DEPARTMENT OF HOME- 
LAND SECURITY.

The Commissioner of U.S. Customs and Border Pro-
tection and the Director of U.S. Immigration and Customs 
Enforcement shall—

(1) designate a principal coordinator within 
U.S. Customs and Border Protection and U.S. Im-
migration and Customs Enforcement, respectively, to 
direct, manage, coordinate, and update their respec-
tive policies and procedures, as well as conduct 
interagency communications, regarding illegally im-
ported cultural property;

(2) update existing directives, regulations, rules, 
and memoranda of understanding of U.S. Customs 
and Border Protection and U.S. Immigration and 
Customs Enforcement, respectively, and, if nec-
essary, devise additional directives, regulations, 
rules, and memoranda of understanding, relating to 
policies and procedures on the illegal importation of 
cultural property in order to—

(A) reflect changes in cultural property 

law, including changes and updates to relevant 
treaties, bilateral agreements, statutes, regula-
tions, and case law that occurred subsequent to 

Customs Directive No. 5230–015, “Customs
Directive on Detention and Seizure of Cultural Property”, dated April 18, 1991;

(B) emphasize investigating, and providing support for investigations and prosecutions, of persons engaged in, conspiring to engage in, or facilitating the illegal importation of cultural property, including smugglers, dealers, buyers, money launderers, and any other appropriate parties; and

(C) provide for communication and coordination between relevant U.S. Customs and Border Protection and U.S. Immigration and Customs Enforcement offices, respectively, in investigating and supporting prosecutions of persons engaged in, conspiring to engage in, or facilitating the illegal importation of cultural property; and

(3) ensure relevant personnel within U.S. Customs and Border Protection and U.S. Immigration and Customs Enforcement, respectively, receive sufficient training in—

(A) relevant cultural property laws;

(B) the identification of cultural property that is at greatest risk of looting and trafficking; and
(C) methods of interdiction and investigative techniques specifically related to illegal trade in cultural property.

SEC. 1304. ROLE OF THE SMITHSONIAN INSTITUTION.

The Secretary of Homeland Security shall ensure that the heads of all components of the Department of Homeland Security involved in cultural property protection activities are authorized to enter into agreements or memoranda of understanding with the Smithsonian Institution to temporarily engage personnel from the Smithsonian Institution for the purposes of furthering such cultural property protection activities.

SEC. 1305. REPORT.

Not later than 1 year after the date of the enactment of this Act and 3 years thereafter, the Commissioner of U.S. Customs and Border Protection and the Commissioner of U.S. Immigration and Customs Enforcement shall jointly submit to the Committee on Ways and Means and the Committee on Homeland Security of the House of Representatives and the Committee on Finance and the Committee on Homeland Security and Governmental Affairs of the Senate a report on—

(1) the progress of the implementation of this Act; and
(2) other actions to enhance and unify efforts to interdict, detain, seize, and investigate cultural property illegally imported into the United States, and investigate, disrupt, and dismantle smuggling and trafficking networks engaged in, conspiring to engage in, or facilitating the illegal importation of cultural property.

TITLE XIV—DEPARTMENT OF HOMELAND SECURITY HEADQUARTERS REFORM AND IMPROVEMENT

SEC. 1401. PROHIBITION ON ADDITIONAL AUTHORIZATION OF APPROPRIATIONS.

No additional funds are authorized to be appropriated to carry out this title and the amendments made by this title. This title and such amendments shall be carried out using amounts otherwise available for such purposes.

Subtitle A—Department of Homeland Security Headquarters Reauthorization

SEC. 1411. DEFINITIONS.

Section 2 of the Homeland Security Act of 2002 is amended—
(1) by redesignating paragraphs (13) through (18) as paragraphs (15) through (20);

(2) by redesignating paragraphs (9) through (12) as paragraphs (10) through (13);

(3) by inserting after paragraph (8) the following:

“(9) The term ‘homeland security enterprise’ means relevant governmental and nongovernmental entities involved in homeland security, including Federal, State, local, and tribal government officials, private sector representatives, academics, and other policy experts.”; and

(4) by inserting after paragraph (13), as so redesignated, the following:

“(14) The term ‘management integration and transformation’—

“(A) means the development of consistent and consolidated functions for information technology, financial management, acquisition management, and human capital management; and

“(B) includes governing processes and procedures, management systems, personnel activities, budget and resource planning, training, real estate management, and provision of secu-
rity, as they relate to functions cited in sub-
paragraph (A).”.

SEC. 1412. HEADQUARTERS COMPONENTS.

(a) IN GENERAL.—Section 102 of the Homeland Se-
curity Act of 2002 (6 U.S.C. 112) is amended—

(1) in subsection (c)—

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

by striking “through the Office of State and
Local Coordination (established under section
801)” and inserting “through the Office of
Partnership and Engagement”;

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

(C) in paragraph (3), by striking the pe-
period and inserting “; and”; and

(D) by adding at the end the following:

“(4) entering into agreements with governments
of other countries, in consultation with the Secretary
of State, and international nongovernmental organi-

cizations in order to achieve the missions of the De-
partment.”; and

(2) by adding at the end the following:

“(h) HEADQUARTERS.—

“(1) COMPONENTS.—The Department Head-
quarters shall include the following:
“(A) The Office of the Secretary.

“(B) The Office of the Deputy Secretary.

“(C) The Executive Secretariat.

“(D) The Management Directorate, including the Office of the Chief Financial Officer.

“(E) The Office of Policy.

“(F) The Office of General Counsel.

“(G) The Office of the Chief Privacy Officer.

“(H) The Office of Civil Rights and Civil Liberties.

“(I) The Office of Operations and Coordination and Planning.

“(J) The Office of Intelligence and Analysis.

“(K) The Office of Legislative Affairs.

“(L) The Office of Public Affairs.

“(2) FUNCTIONS.—The Secretary, through the Headquarters, shall—

“(A) establish the Department’s overall strategy for successfully completing its mission;

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

“(C) establish mechanisms to ensure that components of the Department comply with
Headquarters policies and fully implement the Secretary’s strategies and initiatives and require the head of each component of the Department and component chief officers to comply with such policies and implement such strategies and initiatives;

“(D) establish annual operational and management objectives to determine the Department’s performance;

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

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

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

“(H) manage and encourage shared services across Department components;

“(I) lead and coordinate interaction with Congress and other external organizations; and

“(J) carry out other such functions as the Secretary determines are appropriate.”.
(b) Abolishment of Director of Shared Services.—

(1) Abolishment.—The position of Director of
Shared Services is abolished.

(2) Conforming Amendment.—Section 475
295), and the item relating to such section in the
table of contents in section 1(b) of such Act, are re-
pealed.

(c) Abolishment of the Office of Counter-
narcotics Enforcement.—

(1) Abolishment.—The Office of Counter-
narcotics Enforcement is abolished.

(2) Conforming Amendments.—The Home-
land Security Act of 2002 is amended—

(A) by repealing section 878 (6 U.S.C.
112), and the item relating to that section in
the table of contents in section 1(b) of such
Act; and

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

•HR 6381 IH
SEC. 1413. CHIEF PRIVACY OFFICER.

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

(1) in subsection (a)—

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

(i) by inserting “to be the Chief Privacy Officer of the Department,” after “in the Department,”; and

(ii) by striking “, to assume” and inserting “and who shall have”;

(B) by amending paragraph (6) to read as follows:

“(6) preparing a report to Congress on an annual basis on—

“(A) activities of the Department that affect privacy, including complaints of privacy violations, implementation of section 554 of title 5, United States Code (popularly known as the Privacy Act of 1974), internal controls, and other matters; and

“(B) the number of new technology programs implemented in the Department each fiscal year, the number of those programs that the Chief Privacy Officer has evaluated to ensure that privacy protections are considered and im-
implemented, the number of those programs that
effectively implemented privacy protections into
new technology programs, and an explanation
of why any new programs did not effectively im-
plement privacy protections.”;
(2) by redesignating subsections (b) through (e)
as subsections (e) through (f); and
(3) by inserting after subsection (a) the fol-
lowing:
“(b) ADDITIONAL RESPONSIBILITIES.—In addition
to the responsibilities under subsection (a), the Chief Pri-
vacv Officer shall—
“(1) develop guidance to assist components of
the Department in developing privacy policies and
practices;
“(2) establish a mechanism to ensure such com-
ponents are in compliance with Federal, regulatory,
statutory, and the Department’s privacy require-
ments, mandates, directives, and policy;
“(3) work with the Chief Information Officer of
the Department to identify methods for managing
and overseeing the Department’s records, manage-
ment policies, and procedures;
“(4) work with components and offices of the Department to ensure that information sharing activities incorporate privacy protections;

“(5) serve as the Department’s central office for managing and processing requests related to section 552 of title 5, United States Code, popularly known as the Freedom of Information Act;

“(6) develop public guidance on procedures to be followed when making requests for information under section 552 of title 5, United States Code;

“(7) oversee the management and processing of requests for information under section 552 of title 5, United States Code, within Department Headquarters and relevant Department component offices;

“(8) identify and eliminate unnecessary and duplicative actions taken by the Department in the course of processing requests for information under section 552 of title 5, United States Code; and

“(9) carry out such other responsibilities as the Secretary determines are appropriate, consistent with this section.”; and

(4) by adding at the end the following:

“(g) REASSIGNMENT OF FUNCTIONS.—The Secretary may reassign the functions related to managing and
processing requests for information under section 552 of title 5, United States Code, to another officer within the Department, consistent with requirements of that section.”.

SEC. 1414. OFFICE OF POLICY.

(a) IN GENERAL.—The Homeland Security Act of 2002 (6 U.S.C. 101 et seq.) is amended by—

(1) redesignating section 601 as section 890B, and transferring that section to appear immediately after section 890A; and

(2) striking the heading for title VI and inserting the following:

“TITLE VI—POLICY AND PLANNING

SEC. 601. OFFICE OF POLICY.

“(a) Establishment of Office.—There shall be in the Department an Office of Policy. The Office of Policy shall be headed by an Under Secretary for Policy, who shall be appointed by the President, by and with the advice and consent of the Senate.

“(b) Mission.—The mission of the Office of Policy is to lead, conduct, and coordinate Department-wide policy, strategic planning, and relationships with organizations or persons that are not part of the Department.
“(c) COMPONENTS OF OFFICE.—The Office of Policy shall include the following components:

“(1) The Office of Partnership and Engagement under section 602.

“(2) The Office of International Affairs under section 603.

“(3) The Office of Policy Implementation under section 604.

“(4) The Office of Strategy and Planning under section 605.

“(d) RESPONSIBILITIES OF THE UNDER SECRETARY.—Subject to the direction and control of the Secretary, the Under Secretary for Policy shall—

“(1) serve as the principal policy advisor to the Secretary;

“(2) coordinate with the Under Secretary for Management and the General Counsel of the Department to ensure that development of the Department’s budget is compatible with the priorities, strategic plans, and policies established by the Secretary, including those priorities identified through the Quadrennial Homeland Security Review required under section 707;

“(3) incorporate relevant feedback from, and oversee and coordinate relationships with, organiza-
tions and other persons that are not part of the Department to ensure effective communication of outside stakeholders’ perspectives to components of the Department;

“(4) establish a process to ensure that organizations and other persons that are not part of the Department can communicate with Department components without compromising adherence by the officials of such components to the Department’s ethics and policies;

“(5) manage and coordinate the Department’s international engagement activities;

“(6) advise, inform, and assist the Secretary on the impact of the Department’s policy, processes, and actions on State, local, tribal, and territorial governments;

“(7) oversee the Department’s engagement and development of partnerships with nonprofit organizations and academic institutions;

“(8) administer the Homeland Security Advisory Council and make studies available to the Committee on Homeland Security of the House of Representatives and the Committee on Homeland Security and Governmental Affairs of the Senate on an annual basis; and
“(9) carry out such other responsibilities as the
Secretary determines are appropriate, consistent
with this section.
“(e) COORDINATION BY DEPARTMENT COMPO-
MENTS.—
“(1) IN GENERAL.—To ensure consistency with
the Secretary’s policy priorities, the head of each
component of the Department shall coordinate with
the Office of Policy, as appropriate, in establishing
new policies or strategic planning guidance.
“(2) INTERNATIONAL ACTIVITIES.—
“(A) FOREIGN NEGOTIATIONS.—Each
component of the Department shall coordinate
with the Under Secretary for Policy plans and
efforts of the component before pursuing negoti-
tiations with foreign governments, to ensure
consistency with the Department’s policy prior-
ities.
“(B) NOTICE OF INTERNATIONAL TRAVEL
BY SENIOR OFFICERS.—Each component of the
Department shall notify the Under Secretary
for Policy of the international travel of senior
officers of the Department.
“(f) ASSIGNMENT OF PERSONNEL.—The Secretary
shall assign to the Office of Policy permanent staff and,
as appropriate and consistent with sections 506(c)(2),
821, and 888(d), other appropriate personnel detailed
from other components of the Department to carry out
the responsibilities under this section.

“(g) DEPUTY UNDER SECRETARY FOR POLICY.—

“(1) IN GENERAL.—The Secretary may—

“(A) establish within the Department of Homeland Security a position, to be called the Deputy Under Secretary for Policy, to support the Under Secretary for Policy in carrying out the Under Secretary’s responsibilities; and

“(B) appoint a career employee to such position.

“(2) LIMITATION ON ESTABLISHMENT OF DEPUTY UNDER SECRETARY POSITIONS.—A Deputy Under Secretary position (or any substantially similar position) within the Department of Homeland Security may not be established except for the position provided for by paragraph (1) unless the Secretary of Homeland Security receives prior authorization from Congress.

“(3) DEFINITIONS.—For purposes of paragraph (1)—

“(A) the term ‘career employee’ means any employee (as that term is defined in section
2105 of title 5, United States Code), but does not include a political appointee; and

“(B) the term ‘political appointee’ means any employee who occupies a position which has been excepted from the competitive service by reason of its confidential, policy-determining, policy-making, or policy-advocating character.

SEC. 602. OFFICE OF PARTNERSHIP AND ENGAGEMENT.

“(a) IN GENERAL.—There shall be in the Office of Policy an Office of Partnership and Engagement.

“(b) HEAD OF OFFICE.—The Secretary shall appoint an Assistant Secretary for Partnership and Engagement to serve as the head of the Office.

“(c) RESPONSIBILITIES.—The Assistant Secretary for Partnership and Engagement shall—

“(1) lead the coordination of Department-wide policies relating to the role of State and local law enforcement in preventing, preparing for, protecting against, and responding to natural disasters, acts of terrorism, and other man-made disasters within the United States;

“(2) serve as a liaison between State, local, and tribal law enforcement agencies and the Department, including through consultation with such agencies
regarding Department programs that may impact such agencies;

“(3) coordinate with the Office of Intelligence and Analysis to certify the intelligence and information sharing requirements of State, local, and tribal law enforcement agencies are being addressed;

“(4) work with the Administrator to ensure that law enforcement and terrorism-focused grants to State, local, and tribal government agencies, including grants under sections 2003 and 2004, the Commercial Equipment Direct Assistance Program, and other grants administered by the Department to support fusion centers and law enforcement-oriented programs, are appropriately focused on terrorism prevention activities;

“(5) coordinate with the Science and Technology Directorate, the Federal Emergency Management Agency, the Department of Justice, the National Institute of Justice, law enforcement organizations, and other appropriate entities to support the development, promulgation, and updating, as necessary, of national voluntary consensus standards for training and personal protective equipment to be used in a tactical environment by law enforcement officers;
“(6) create and foster strategic communications with the private sector to enhance the primary mission of the Department to protect the American homeland;

“(7) advise the Secretary on the impact of the Department’s policies, regulations, processes, and actions on the private sector;

“(8) interface with other relevant Federal agencies with homeland security missions to assess the impact of these agencies’ actions on the private sector;

“(9) create and manage private sector advisory councils composed of representatives of industries and associations designated by the Secretary to—

“(A) advise the Secretary on private sector products, applications, and solutions as they relate to homeland security challenges;

“(B) advise the Secretary on homeland security policies, regulations, processes, and actions that affect the participating industries and associations; and

“(C) advise the Secretary on private sector preparedness issues, including effective methods for—
“(i) promoting voluntary preparedness standards to the private sector; and

“(ii) assisting the private sector in adopting voluntary preparedness standards;

“(10) promote existing public-private partnerships and developing new public-private partnerships to provide for collaboration and mutual support to address homeland security challenges;

“(11) assist in the development and promotion of private sector best practices to secure critical infrastructure;

“(12) provide information to the private sector regarding voluntary preparedness standards and the business justification for preparedness and promoting to the private sector the adoption of voluntary preparedness standards;

“(13) coordinate industry efforts, with respect to functions of the Department of Homeland Security, to identify private sector resources and capabilities that could be effective in supplementing Federal, State, and local government agency efforts to prevent or respond to a terrorist attack;

“(14) coordinate with the Commissioner of Customs and Border Protection and the appropriate
senior official of the Department of Commerce on
issues related to the travel and tourism industries;

“(15) coordinate the activities of the Depart-
ment relating to State and local government;

“(16) assess, and advocate for, the resources
needed by State and local governments to implement
the national strategy for combating terrorism;

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

“(18) develop a process for receiving meaning-
ful input from State and local governments to assist
the development of the national strategy for com-
bating terrorism and other homeland security activi-
ties; and

“(19) perform such other functions as are es-
tablished by law or delegated to such Assistant Sec-
retary by the Under Secretary for Policy.

“SEC. 603. OFFICE OF INTERNATIONAL AFFAIRS.

“(a) In General.—There shall be in the Office of
Policy an Office of International Affairs.

“(b) Head of Office.—The Secretary shall appoint
an Assistant Secretary for International Affairs to serve
as the head of the Office and as the chief diplomatic offi-
cer of the Department.
“(c) FUNCTIONS.—

“(1) IN GENERAL.—The Assistant Secretary for International Affairs shall—

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

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

“(C) develop, in consultation with the Under Secretary for Management, guidance for selecting, assigning, training, and monitoring overseas deployments of Department personnel, including minimum standards for predeployment training;

“(D) develop and update, in coordination with all components of the Department engaged in international activities, a strategic plan for the international activities of the Department,
establish a process for managing its implementation, and establish mechanisms to monitor the alignment between assets, including personnel, deployed by the Department outside the United States and the plan required by this subparagraph;

“(E) develop and distribute guidance on Department policy priorities for overseas activities to personnel deployed overseas, that, at a minimum, sets forth the regional and national priorities being advanced by their deployment, and establish mechanisms to foster better coordination of Department personnel, programs, and activities deployed outside the United States;

“(F) maintain awareness regarding the international travel of senior officers of the Department and their intent to pursue negotiations with foreign government officials, and review resulting draft agreements;

“(G) develop, in consultation with the components of the Department, including, as appropriate, with the Under Secretary for the Science and Technology Directorate, programs to support the overseas programs conducted by the
Department, including training, technical assistance, and equipment to ensure that Department personnel deployed abroad have proper resources and receive adequate and timely support;

“(H) conduct the exchange of homeland security information, in consultation with the Under Secretary of the Office of Intelligence and Analysis, and best practices relating to homeland security with foreign nations that, in the determination of the Secretary, reciprocate the sharing of such information in a substantially similar manner;

“(I) submit information to the Under Secretary for Policy for oversight purposes, including preparation of the quadrennial homeland security review and on the status of overseas activities, including training and technical assistance and information exchange activities and the Department’s resources dedicated to these activities;

“(J) promote, when appropriate, and oversee the exchange of education, training, and information with nations friendly to the United
States in order to share best practices relating to homeland security; and

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

“(2) INVENTORY OF ASSETS DEPLOYED ABROAD.—For each fiscal year, the Assistant Secretary for International Affairs, in coordination with the Under Secretary for Management, shall provide to the Committee on Homeland Security of the House of Representatives and the Committee on Homeland Security and Governmental Affairs of the Senate with the annual budget request for the Department, an annual accounting of all assets of the Department, including personnel, deployed outside the United States on behalf of the Department.

“(3) STANDARDIZED FRAMEWORK FOR COST DATA.—The Assistant Secretary for International Affairs shall utilize a standardized framework to collect and maintain comparable cost data for all assets of the Department, including personnel, deployed outside the United States to prepare the annual accounting required by paragraph (2).

“(4) EXCLUSIONS.—This subsection does not apply to international activities related to the protec-
tive mission of the United States Secret Service, or
to the Coast Guard when operating under the direct
authority of the Secretary of Defense or the Sec-
retary of the Navy.

"SEC. 604. OFFICE OF POLICY IMPLEMENTATION.

"(a) In General.—There shall be in the Office of
Policy an Office of Policy Implementation.

"(b) Head of Office.—The Secretary shall appoint
a Director of the Office of Policy Implementation to serve
as the head of the Office.

"(c) Responsibilities.—The Director of the Office
of Policy Implementation shall lead, conduct, coordinate,
and provide overall direction and supervision of Depart-
ment-wide policy development for the programs, offices,
and activities of the Department, in consultation with rel-
evant officials of the Department, to ensure quality, con-
sistency, and integration across the Department, as appro-
priate.

"SEC. 605. OFFICE OF STRATEGY AND PLANNING.

"(a) In General.—There shall be in the Office of
Policy of the Department an Office of Strategy and Plan-
ning.

"(b) Head of Office.—The Secretary shall appoint
a Director of the Office of Strategy and Planning who
shall serve as the head of the Office.
“(c) Responsibilities.—The Director of the Office of Strategy and Planning shall—

“(1) lead and conduct long-term Department-wide strategic planning, including the Quadrennial Homeland Security Review and planning guidance for the Department, and translate the Department’s statutory responsibilities, strategic plans, and long-term goals into risk-based policies and procedures that improve operational effectiveness; and

“(2) develop strategies to address unconventional threats to the homeland.”.

(b) Clerical Amendment.—The table of contents in section 1(b) of such Act is amended—

(1) by striking the items relating to title VI and inserting the following:

“TITLE VI—POLICY AND PLANNING

Sec. 601. Office of Policy.
Sec. 602. Office of Partnership and Engagement.
Sec. 603. Office of International Affairs.
Sec. 604. Office of Policy Implementation.
Sec. 605. Office of Strategy and Planning.”.

(2) by inserting after the item relating to section 890A the following:

“Sec. 890B. Treatment of charitable trusts for members of the Armed Forces of the United States and other governmental organizations.”.

(c) Appointment of Under Secretary for Policy; Continuation of Service of Assistant Secretary.—
(1) **TIME OF APPOINTMENT.**—The President may appoint an Under Secretary for Policy under section 601 of the Homeland Security Act of 2002, as amended by this title, only on or after January 20, 2017.

(2) **HEAD OF OFFICE PENDING APPOINTMENT.**—The individual serving as the Assistant Secretary for Policy of the Department of Homeland Security on the date of the enactment of this Act, or their successor, may continue to serve as an Assistant Secretary and as the head of the Office of Policy established by such section, until the date on which the Under Secretary for Policy is appointed under such section in accordance with paragraph (1).

(d) **APPOINTMENT OF ASSISTANT SECRETARY FOR INTERNATIONAL AFFAIRS; ABOLISHMENT OF EXISTING OFFICE.**—

(1) **TIME OF APPOINTMENT.**—The Secretary of Homeland Security may appoint an Assistant Secretary for International Affairs under section 602 of the Homeland Security Act of 2002, as amended by this title, only on or after January 20, 2017.

(2) **HEAD OF OFFICE PENDING APPOINTMENT.**—The individual serving as the Assistant Sec-
retary for International Affairs of the Department of Homeland Security on the date of the enactment of this Act, or their successor, may continue to serve as a Deputy Assistant Secretary and as the head of the Office of International Affairs established by such section, until the date the Under Secretary for Policy is appointed under such section in accordance with paragraph (1).

(3) ABOLISHMENT OF EXISTING OFFICE.—

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

(B) TRANSFER OF ASSETS AND PERSONNEL.—The assets and personnel associated with such Office are transferred to the head of the Office of International Affairs provided for by section 603 of the Homeland Security Act of 2002, as amended by this title.

(C) CONFORMING AMENDMENT.—Subsection 879 of the Homeland Security Act of 2002 (6 U.S.C. 459), and the item relating to such section in section 1(b) of such Act, are repealed.

(e) ABOLISHMENT OF OFFICE FOR STATE AND LOCAL LAW ENFORCEMENT.—
(1) IN GENERAL.—The Office for State and Local Law Enforcement of the Department of Homeland Security is abolished.

(2) TRANSFER OF FUNCTIONS, ASSETS, AND PERSONNEL.—The functions authorized to be performed by such office immediately before the enactment of this Act, and the assets and personnel associated with such functions, are transferred to the head of the Office of Partnership and Engagement provided for by section 602 of the Homeland Security Act of 2002, as amended by this title.

(3) CONFORMING AMENDMENT.—Subsection (b) of section 2006 of the Homeland Security Act of 2002 (6 U.S.C. 607) is repealed.

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

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

(2) TRANSFER OF FUNCTIONS AND ASSETS.—The functions authorized to be performed by such office immediately before the enactment of this Act, and the assets and personnel associated with such functions, are transferred to the head of Office of Partnership and Engagement provided for by section

(3) CONFORMING AMENDMENTS.—Section 801 of the Homeland Security Act of 2002 (6 U.S.C. 631), and the item relating to that section in the table of contents in section 1(b) of such Act, are repealed.

(g) ABOLISHMENT OF SPECIAL ASSISTANT TO THE SECRETARY.—

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

(2) TRANSFER OF FUNCTIONS AND ASSETS.—The functions authorized to be performed by such Special Assistant to the Secretary immediately before the enactment of this Act, and the assets and personnel associated with such functions, are transferred to the head of the Office of Partnership and Engagement provided for by section 602 of the Homeland Security Act of 2002, as amended by this title.
(3) CONFORMING AMENDMENT.—Section 102(f) of the Homeland Security Act of 2002 (6 U.S.C. 112(f)) is repealed.

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

(1) in paragraph (1), by striking subparagraph (I) and redesignating subparagraph (J) as subparagraph (I); and

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

“(2) ASSISTANT SECRETARIES.—

“(A) ADVICE AND CONSENT APPOINTMENTS.—The Department shall have the following Assistant Secretaries appointed by the President, by and with the advice and consent of the Senate:

“(i) The Assistant Secretary, U.S. Immigration and Customs Enforcement.

“(ii) The Assistant Secretary, Transportation Security Administration.

“(B) OTHER PRESIDENTIAL APPOINTMENTS.—The Department shall have the following Assistant Secretaries appointed by the President:
“(i) The Assistant Secretary, Infrastructure Protection.

“(ii) The Assistant Secretary, Office of Public Affairs.

“(iii) The Assistant Secretary, Office of Legislative Affairs.

“(C) SECRETARIAL APPOINTMENTS.—The Department shall have the following Assistant Secretaries appointed by the Secretary:

“(i) The Assistant Secretary, Office of Cybersecurity and Communications.

“(ii) The Assistant Secretary for International Affairs under section 602.

“(iii) The Assistant Secretary for Partnership and Engagement under section 603.

“(D) LIMITATION ON CREATION OF POSITIONS.—No Assistant Secretary position may be created in addition to the positions provided for by this section unless such position is authorized by a statute enacted after the date of the enactment of the DHS Headquarters Reform and Improvement Act of 2015.”.

(i) HOMELAND SECURITY ADVISORY COUNCIL.—Section 102(b) of the Homeland Security Act of 2002 (6
U.S.C. 112(b)) is amended by striking “and” after the semicolon at the end of paragraph (2), striking the period at the end of paragraph (3) and inserting “; and”, and adding at the end the following:

“(4) shall establish a Homeland Security Advisory Council to provide advice and recommendations on homeland-security-related matters.”.

(j) Prohibition on New Offices.—No new office may be created to perform functions transferred by this section, other than as provided in section 601 of the Homeland Security Act of 2002, as amended by this title, unless the Secretary of Homeland Security receives prior authorization from Congress permitting such change.

(k) Definitions.—In this section each of the terms “functions”, “assets”, and “personnel” has the meaning that term has under section 2 of the Homeland Security Act of 2002 (6 U.S.C. 101).

(l) Duplication Review.—The Secretary of Homeland Security shall—

(1) within 1 year after the date of the enactment of this Act, complete a review of the international affairs offices, functions, and responsibilities of the components of the Department of Homeland Security, to identify and eliminate areas of unnecessary duplication; and
(2) within 30 days after the completion of such review, provide the results of the review to the Committee on Homeland Security of the House of Representatives and the Committee on Homeland Security and Governmental Affairs of the Senate.

SEC. 1415. QUADRENNIAL HOMELAND SECURITY REVIEW.


(1) in subsection (a)—

(A) by amending paragraph (1) to read as follows:

“(1) Review required.—In fiscal year 2017, and every 4 years thereafter, the Secretary shall conduct a review of the homeland security of the Nation (in this section referred to as a ‘quadrennial homeland security review’). Such review shall be conducted so that it is completed, and the report under subsection (c) is issued, by no later than December 31, 2017, and by December 31 of every fourth year thereafter.”; and

(B) in paragraph (3) by striking “The Secretary shall conduct each quadrennial homeland security review under this subsection in consultation with” and inserting “In order to ensure that each quadrennial homeland security
review conducted under this section is coordinated with the quadrennial defense review conducted by the Secretary of Defense under section 118 of title 10, United States Code, and any other major strategic review relating to diplomacy, intelligence, or other national security issues, the Secretary shall conduct and obtain information and feedback from entities of the homeland security enterprise through”;

(2) in subsection (b)—

(A) in paragraph (5), by striking “and” after the semicolon at the end;

(B) in paragraph (6), by striking the period and inserting “; and”; and

(C) by adding after paragraph (6) the following:

“(7) leverage analytical tools and resources developed as part of the quadrennial homeland security review to support the Department’s ongoing programs and missions.”;

(3) in subsection (c)(2)—

(A) by striking “and” after the semicolon at the end of subparagraph (H);

(B) by redesignating subparagraph (I) as subparagraph (L); and
(C) by inserting after subparagraph (H) the following:

“(I) a description of how the conclusions under the quadrennial homeland security review will inform efforts to develop capabilities and build capacity of States, local governments, Indian tribes, and private entities, and of individuals, families, and communities;

“(J) as appropriate, proposed changes to the authorities, organization, governance structure, or business processes (including acquisition processes) of the Department in order to better fulfill responsibilities of the Department;

“(K) where appropriate, a classified annex, including materials prepared pursuant to section 306 of title 5, United States Code, relating to the preparation of an agency strategic plan, to satisfy, in whole or in part, the reporting requirements of this paragraph; and”.

SEC. 1416. FUTURE YEARS HOMELAND SECURITY PROGRAM.


(1) by amending subsection (a) to read as follows:
“(a) IN GENERAL.—Not later than the 30 days following the date of each fiscal year on which the budget of the President is submitted to Congress under section 1105(a) of title 31, United States Code, the Secretary shall submit to the Committee on Homeland Security of the House of Representatives and the Committee on Homeland Security and Governmental Affairs of the Senate a Future Years Homeland Security Program that provides detailed estimates of the projected expenditures and corresponding requests for appropriations included in that budget. The Future Years Homeland Security Program shall cover the fiscal year for which the budget is submitted and the 4 succeeding fiscal years.”; and

(2) by adding at the end the following:

“(d) CONSISTENCY OF BUDGET REQUEST WITH ESTIMATES.—For each fiscal year, the Secretary shall ensure that the projected amounts specified in program and budget information for the Department submitted to Congress in support of the President’s budget request are consistent with the estimated expenditures and proposed appropriations necessary to support the programs, projects, and activities of the Department included in the budget pursuant to section 1105(a)(5) of title 31, United States Code.
“(e) EXPLANATION OF ALIGNMENT WITH STRATEGIES AND PLANS.—Together with the detailed estimates of the projected expenditures and corresponding requests for appropriations submitted for the Future Years Homeland Security Program, the Secretary shall provide an explanation of how those estimates and requests align with the homeland security strategies and plans developed and updated as appropriate by the Secretary. Such explanation shall include an evaluation of the organization, organizational structure, governance structure, and business processes (including acquisition processes) of the Department, to ensure that the Department is able to meet its responsibilities.

“(f) PROJECTION OF ACQUISITION ESTIMATES.—Each Future Years Homeland Security Program shall project—

“(1) acquisition estimates for a period of 5 fiscal years, with specified estimates for each fiscal year, for major acquisition programs by the Department and each component therein, including modernization and sustainment expenses; and

“(2) estimated annual deployment schedules for major acquisition programs over the 5-fiscal-year period.
“(g) CONTINGENCY AMOUNTS.—Nothing in this section shall be construed as prohibiting the inclusion in the Future Years Homeland Security Program of amounts for management contingencies, subject to the requirements of subsection (b).

“(h) CLASSIFIED OR SENSITIVE ANNEX.—The Secretary may include with each submission under this section a classified or sensitive annex containing any information required to be submitted under this section that is restricted from public disclosure in accordance with Federal law, including information that is determined to be Sensitive Security Information under section 537 of the Department of Homeland Security Appropriations Act, 2006 (6 U.S.C. 114) to Congress in a classified or sensitive annex.

“(i) AVAILABILITY OF INFORMATION TO THE PUBLIC.—The Secretary shall make available to the public in electronic form the information required to be submitted to Congress under this section, other than information described in subsection (h).”.

SEC. 1417. MANAGEMENT AND EXECUTION.

Section 701 of the Homeland Security Act of 2002 (6 U.S.C. 341) is amended by striking subsections (a) and (b) and inserting the following:
“(a) IN GENERAL.—Subject to the direction and control of the Secretary, the Under Secretary for Management shall serve as the following:

“(1) The Chief Management Officer for all matters related to the management and administration of the Department in support of homeland security operations and programs. With regard to the management functions for which the Under Secretary has responsibility by law or by direction of the Secretary, the Under Secretary for Management takes precedence in the Department after the Secretary and the Deputy Secretary of Homeland Security.

“(2) The senior official with the authority to administer, implement, and direct management integration and transformation across functional disciplines of the Department, including—

“(A) information technology, financial management, acquisition management, and human capital management of the Department to improve program efficiency and effectiveness;

“(B) ensure compliance with laws, rules, regulations, and the Department’s policies;

“(C) conduct regular oversight; and

“(D) prevent unnecessary duplication of programs in the Department.
“(b) Responsibilities.—In addition to responsibilities designated by the Secretary or otherwise established by law, the Under Secretary for Management shall be responsible for performing, or delegating responsibility for performing, the following activities of the Department:

“(1) Development of the budget, management of appropriations, expenditures of funds, accounting, and finance.

“(2) Acquisition and procurement activities under section 701(d).

“(3) Human resources and personnel.

“(4) Information technology and communication systems, in consultation with the Under Secretary for Intelligence and Analysis, as appropriate.

“(5) Facilities, property, equipment, and other material resources.

“(6) Real property and personal property.

“(7) Security for personnel, information technology and communications systems, facilities, property, equipment, and other material resources.

“(8) Strategic management planning, annual performance planning, and identification and tracking of performance measures relating to the responsibilities of the Department, including such respon-
sibilities under section 306 of title 5, United States Code.

“(9) Oversight of grants and other assistance management programs to ensure proper administra-

“(10) Management integration and trans-
formation within each functional management disci-
pline of the Department, including information technology, financial management, acquisition man-
agement, and human capital management, and the transition process, to ensure an efficient and orderly consolidation of functions and personnel in the De-
partment and transition, including the—

“(A) development of coordinated data sources and connectivity of information systems to the greatest extent practical to enhance pro-
gram visibility and transparency;

“(B) development of standardized, auto-
mated, and real-time management information to uniformly manage and oversee programs, and make informed decisions to improve the ef-
ficiency of the Department;

“(C) development of effective program management and regular oversight mechanisms,

including clear roles and processes for program
governance, sharing of best practices, and access to timely, reliable, and analyzed data on all acquisitions and investments;

“(D) implementation of mechanisms to promote accountability for management integration among Department and component chief officers;

“(E) integration of financial management systems within and across the Department to ensure financial transparency, support daily operational and financial decisionmaking, and maintain consecutive unqualified opinions for all financial statements, including the responsibility to review, approve, and oversee the planning, design, acquisition, deployment, operation, maintenance, and modernization of business systems;

“(F) integration of human resource management systems within and across the Department to track and record information (including attrition rates, knowledge, skills, and abilities critical for workforce planning, identifying current and future human capital needs, including recruitment efforts and improving employee morale), including the responsibility to review, ap-
prove, and oversee the planning, design, acquisition, deployment, operation, maintenance, and modernization of business systems;

“(G) development of a management integration strategy for the Department and its components to be submitted annually with the President’s budget to ensure that management of the Department is strengthened in the areas of human capital, acquisition, information technology, and financial management, which shall include—

“(i) short- and long-term objectives to effectively guide implementation of interoperable business systems solutions;

“(ii) issuance of guidance and action plans with dates, specific actions, and costs for implementing management integration and transformation of common functional disciplines across the Department and its components;

“(iii) specific operational and tactical goals, activities, and timelines needed to accomplish the integration effort;

“(iv) performance measures to monitor and validate corrective measures;
“(v) efforts to identify resources needed to achieve key actions and outcomes;

“(vi) other issues impeding management integration;

“(vii) reporting to the Government Accountability Office twice annually to demonstrate measurable, sustainable progress made in implementing the Department’s corrective action plans and achieving key outcomes, including regarding—

“(I) leadership commitment;

“(II) capacity building; and

“(III) continuous monitoring to address Government Accountability Office designations of programs at high risk for waste, fraud, and abuse, including with respect to strengthening management functions;

“(viii) review and approve any major update to the Department’s strategy related to management integration and transformation across functional disciplines and lines of business, including any business systems modernization plans to maxi-
mize benefits and minimize costs for the
Department; and

“(ix) before December 1 of each year
in which a Presidential election is held, the
development of a transition and succession
plan to guide the transition of Department
functions to a new Presidential administra-
tion, and making such plan available to the
next Secretary and Under Secretary for
Management and to the homeland security
congressional committees.

“(H) Oversight, including the conduct of
internal audits and management analyses, of
the programs and activities of the Department.
Such supervision includes establishing oversight
procedures to ensure a full and effective review
of the efforts by Department components to im-
plement policies and procedures of the Depart-
ment for management integration and trans-
formation.

“(I) Any other management duties that
the Secretary may designate.”.

SEC. 1418. CHIEF FINANCIAL OFFICER.

Section 702 of the Homeland Security Act of 2002
(6 U.S.C. 341) is amended by redesignating subsections
(b) and (c) as subsections (c) and (d), respectively, and by inserting after subsection (a) the following:

“(b) RESPONSIBILITIES.—Notwithstanding sections 901 and 1122 of title 31, United States Code, the Chief Financial Officer, in consultation with the Under Secretary for Management and the Under Secretary for Intelligence and Analysis, as appropriate, shall—

“(1) lead cost-estimating practices for the Department, including the development of the Department’s policy on cost estimating and approval of life cycle cost estimates;

“(2) oversee coordination with the Office of Policy on the Department’s long-term strategic planning to ensure that the development of the Department’s budget is compatible with the priorities, strategic plans, and policies established by the Secretary;

“(3) develop and oversee the Department’s financial management policy;

“(4) provide guidance for and over financial system modernization efforts throughout the Department;

“(5) establish effective internal controls over financial reporting systems and processes throughout the Department;
“(6) lead assessments of internal controls related to the Department’s financial management systems and review financial processes to ensure that internal controls are designed properly and operate effectively;

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

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

“(9) ensure that Department components’ senior financial officers certify that their major acquisition programs have adequate resources to execute their programs through the 5-year future years homeland security program period, so that the Department’s funding requirements for major acquisition programs match expected resources;

“(10) ensure that components identify and report all expected costs of acquisition programs to the Chief Financial Officer of the Department;

“(11) oversee Department budget formulation and execution;
“(12) fully implement a common accounting structure to be used across the entire Department by fiscal year 2019; and

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

“(A) report to the Inspector General of the Department the expenditures by the component for each conference hosted or attended by Department employees for which the total expenditures of the Department exceed $20,000, within 15 days after the date of the conference; and

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

“(i) the information described in subsections (a), (b), and (c) of section 739 of Public Law 113–235; and

“(ii) documentation of such expenditures.”.

SEC. 1419. CHIEF PROCUREMENT OFFICER.

(a) IN GENERAL.—Title VII of the Homeland Security Act of 2002 (6 U.S.C. 341 et seq.) is further amended by adding at the end the following:
“SEC. 708. CHIEF PROCUREMENT OFFICER.

“(a) IN GENERAL.—There is a Chief Procurement Officer of the Department, who shall report directly to the Under Secretary for Management. The Chief Procurement Officer is the senior procurement executive for purposes of section 1702(c) of title 41 United States Code, and shall perform procurement functions as specified in such section. The Chief Procurement Officer also shall perform other functions and responsibilities set forth in this section and as may be assigned by the Under Secretary for Management.

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

“(1) exercise leadership and authority to the extent delegated by the Under Secretary for Management over the Department’s procurement function;

“(2) issue procurement policies, and shall serve as a senior business advisor to agency officials on acquisition-related matters, including policy and workforce matters, as determined by the Under Secretary for Management;

“(3) account for the integrity, performance, and oversight of Department procurement and contracting functions and be responsible for ensuring that a procurement’s contracting strategy and plans
are consistent with the intent and direction of the
Acquisition Review Board;

“(4) serve as the Department’s main liaison to
industry on procurement-related issues;

“(5) oversee a centralized certification and
training program, in consultation with the Under
Secretary for Management, for the entire Depart-
ment acquisition workforce while using, to the great-
est extent practicable, best practices and acquisition
training opportunities already in existence within the
Federal Government, the private sector, or univer-
sities and colleges, as appropriate, and including
training on how best to identify actions that warrant
referrals for suspension or debarment;

“(6) delegate or retain contracting authority, as
appropriate;

“(7) provide input on the periodic performance
reviews of each head of contracting activity of the
Department;

“(8) collect baseline data and use such data to
establish performance measures on the impact of
strategic sourcing initiatives on the private sector,
including, in particular, small businesses;

“(9) ensure that a fair proportion (as defined
pursuant to the Small Business Act (15 U.S.C. 631
et seq.) of Federal contract and subcontract dollars are awarded to small businesses, maximize opportunities for small business participation, and ensure, to the extent practicable, small businesses that achieve qualified vendor status for security-related technologies are provided an opportunity to compete for contracts for such technology; and

“(10) conduct oversight of implementation of administrative agreements to resolve suspension or debarment proceedings and, upon request, provide information to the Committee on Homeland Security of the House of Representatives and the Committee on Homeland Security and Governmental Affairs of the Senate about the effectiveness of such agreements at improving contractor responsibility.

“(c) HEAD OF CONTRACTING ACTIVITY DEFINED.—

In this section the term ‘head of contracting activity’ means each official responsible for the creation, management, and oversight of a team of procurement professionals properly trained, certified, and warranted to accomplish the acquisition of products and services on behalf of the designated components, offices, and organizations of the Department, and as authorized, other government entities.”.
(b) CLERICAL AMENDMENT.—The table of contents in section 1(b) of such Act is further amended by adding at the end of the items relating to such title the following:

“Sec. 708. Chief Procurement Officer.”.

SEC. 1420. CHIEF INFORMATION OFFICER.

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

(1) in subsection (a), by adding at the end the following: “In addition to the functions under section 3506(a)(2) of title 44, United States Code, the Chief Information Officer shall perform the functions set forth in this section and such other functions as may be assigned by the Secretary.”;

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

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

“(b) RESPONSIBILITIES.—In addition to the functions under section 3506 of title 44, United States Code, the Chief Information Officer, in consultation with the Under Secretary for Management, shall—

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

“(2) to the extent delegated by the Secretary—

“(A) exercise leadership and authority over
Department information technology manage-
ment; and

“(B) establish the information technology
priorities, policies, processes, standards, guide-
lines, and procedures of the Department to en-
sure interoperability and standardization of in-
formation technology;

“(3) serve as the lead technical authority for in-
formation technology programs;

“(4) maintain a consolidated inventory of the
Department’s mission critical and mission essential
information systems, and develop and maintain con-
tingency plans for responding to a disruption in the
operation of any of those information systems;

“(5) maintain the security, visibility, reliability,
integrity, and availability of data and information
technology of the Department including the security
of the Homeland Security Data Network;

“(6) in coordination with relevant officials of
the Department, ensure that the Department is in
compliance with subchapter II of chapter 35 of title 44, United States Code;

“(7) establish policies and procedures to effectively monitor and manage vulnerabilities in the supply chain for purchases of information technology;

“(8) in coordination with relevant officials of the Department, ensure Department compliance with Homeland Security Presidential Directive 12;

“(9) in coordination with relevant officials of the Department, ensure that information technology systems of the Department meet the standards established under the information sharing environment, as defined in section 1016 of the Intelligence Reform and Terrorism Prevention Act of 2004 (6 U.S.C. 485);

“(10) develop measures to monitor the performance of Department components’ use and implementation of information technology systems and consistently monitor such performance to ensure that such systems are used effectively;

“(11) ensure that Department components report to the Chief Information Officer of the Department a complete inventory of information systems and fully adhere to Department guidance related to information technology;
“(12) carry out any other responsibilities delegated by the Secretary consistent with an effective information system management function; and

“(13) carry out authorities over Department information technology consistent with section 113419 of title 40, United States Code.

“(c) STRATEGIC PLANS.—In coordination with the Chief Financial Officer, the Chief Information Officer shall develop an information technology strategic plan every 5 years and report to the Committee on Homeland Security and the Committee on Appropriations of the House of Representatives and the Committee on Homeland Security and Governmental Affairs and the Committee on Appropriations of the Senate on—

“(1) how the information technology strategic plans developed under this subsection are used to help inform the Department’s budget process;

“(2) how the Department’s budget aligns with priorities specified in the information technology strategic plans;

“(3) in cases in which it is not possible to fund all information technology strategic plan activities for a given fiscal year, the rationale as to why certain activities are not being funded in lieu of higher priorities;
“(4) what decisionmaking process was used to arrive at these priorities and the role of Department components in that process; and

“(5) examine the extent to which unnecessary duplicate information technology within and across the components of the Department has been eliminated.

“(d) SOFTWARE LICENSING.—

“(1) IN GENERAL.—Not later than 180 days after the date of the enactment of the DHS Headquarters Reform and Improvement Act of 2015, and every 2 years thereafter until 2020, the Chief Information Officer, in consultation with Department component chief information officers, shall—

“(A) conduct a Department-wide inventory of all existing software licenses held by the Department, including utilized and unutilized licenses;

“(B) assess the needs of the Department and the components of the Department for software licenses for the subsequent 2 fiscal years;

“(C) examine how the Department can achieve the greatest possible economies of scale and cost savings in the procurement of software licenses;
“(D) determine how the use of shared cloud-computing services will impact the needs for software licenses for the subsequent 2 fiscal years; and

“(E) establish plans and estimated costs for eliminating unutilized software licenses for the subsequent 2 fiscal years.

“(2) EXCESS SOFTWARE LICENSING.—

“(A) PLAN TO REDUCE SOFTWARE LICENSES.—If the Chief Information Officer determines through the inventory conducted under paragraph (1) that the number of software licenses held by the Department and the components of the Department exceed the needs of the Department as assessed under paragraph (1), the Secretary, not later than 90 days after the date on which the inventory is completed, shall establish a plan for bringing the number of such software licenses into balance with such needs of the Department.

“(B) PROHIBITION ON PROCUREMENT OF NEW SOFTWARE LICENSES.—

“(i) IN GENERAL.—Except as provided in clause (ii), upon completion of a plan established under paragraph (1), no
additional resources may be obligated for
the procurement of new software licenses
for the Department until such time as the
need of the Department exceeds the num-
ber of used and unused licenses held by the
Department.

“(ii) Exception.—The Chief Infor-
mation Officer may authorize the purchase
of additional licenses and amend the num-
ber of needed licenses as necessary.

“(3) GAO Review.—The Comptroller General
of the United States shall review the inventory con-
ducted under paragraph (1)(A) and the plan estab-
ilished under paragraph (2)(A).

“(4) Submission to Congress.—The Chief
Information Officer shall submit a copy of each in-
ventory conducted under paragraph (1)(A) and each
plan established under paragraph (2)(A) to the
Committee on Homeland Security of the House of
Representatives and the Committee on Homeland
Security and Governmental Affairs of the Senate.”.

(b) Completion of First Definition of Capa-
bilities.—The Chief Information Officer shall complete
the first implementation of section 701(c) of the Home-
land Security Act of 2002, as amended by this section,
by not later than 1 year after the date of the enactment of this Act.

SEC. 1421. CHIEF HUMAN CAPITAL OFFICER.

Section 704 of the Homeland Security Act of 2002 (6 U.S.C. 343) is amended to read as follows:

```
SEC. 704. CHIEF HUMAN CAPITAL OFFICER.

(a) IN GENERAL.—There is a Chief Human Capital Officer of the Department who shall report directly to the Under Secretary of Management.

(b) RESPONSIBILITIES.—The Chief Human Capital Officer shall—

(1) develop and implement strategic workforce planning efforts that are consistent with Government-wide leading principles, and that are in line with Department strategic human capital goals and priorities;

(2) develop performance measures to provide a basis for monitoring and evaluating Department-wide strategic workforce planning efforts;

(3) develop strategies to recruit, hire, and train the Department workforce;

(4) work with the component heads to identify methods for managing and overseeing human capital programs and initiatives;
```
“(5) develop a career path framework, and create opportunities for leader development;

“(6) serve as the Department’s central office for managing employee resources, including training and development opportunities;

“(7) coordinate the Department’s human resource management system;

“(8) conduct efficiency reviews to determine if components are implementing human capital programs and initiatives; and

“(9) identify and eliminate unnecessary and duplicative human capital policies and guidance.

“(c) COMPONENT STRATEGIES.—

“(1) IN GENERAL.—Each component of the Department shall coordinate with the Chief Human Capital Officer of the Department to develop or maintain its own 5-year workforce strategy that will support the Department’s goals, objectives, performance measures, and determination of the proper balance of Federal employees and private labor resources.

“(2) STRATEGY REQUIREMENTS.—The Chief Human Capital Officer shall ensure that, in the development of the strategy required by subsection (c), the head of the component reports to the Chief
Human Capital Officer on the human resources considerations associated with creating additional Federal full-time equivalent positions, converting private contractor positions to Federal employee positions, or relying on the private sector for goods and services, including—

“(A) hiring projections, including occupation and grade level, as well as corresponding salaries, benefits, and hiring or retention bonuses;

“(B) the identification of critical skills requirements over the 5-year period, any current or anticipated need for critical skills required at the Department, and the training or other measures required to address such need;

“(C) recruitment of qualified candidates and retention of qualified employees;

“(D) supervisory and management requirements;

“(E) travel and related personnel support costs;

“(F) the anticipated cost and impact on mission performance associated with replacing Federal personnel due to their retirement or other attrition; and
“(G) other appropriate factors.

“(d) **ANNUAL SUBMISSION.**—The Secretary shall provide to the appropriate congressional committees, together with submission of the annual budget justification, information on the progress within the Department of fulfilling the workforce strategies required under subsection (e).”.

**SEC. 1422. CHIEF SECURITY OFFICER.**

(a) **IN GENERAL.**—Title VII of the Homeland Security Act of 2002 (6 U.S.C. 341 et seq.), as amended by section 1619(a) of this title, is further amended by adding at the end the following:

```
```

**SEC. 709. CHIEF SECURITY OFFICER.**

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

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

“(1) develop and implement the Department’s security policies, programs, and standards;

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

“(3) provide support to Department components on security-related matters.”.
(b) CLERICAL AMENDMENT.—The table of contents in section 1(b) of such Act is further amended by adding at the end of the items relating to such title the following:

“Sec. 709. Chief Security Officer.”.

SEC. 1423. COST SAVINGS AND EFFICIENCY REVIEWS.

Not later than 1 year after the date of the enactment of this Act, the Secretary of Homeland Security, acting through the Under Secretary for Management of the Department of Homeland Security, shall submit to the Committee on Homeland Security of the House of Representatives and the Committee on Homeland Security and Governmental Affairs of the Senate a report that—

(1) provides a detailed inventory of the management and administrative expenditures and activities of the components of the Department and identifies potential cost savings and efficiencies for those expenditures and activities of each such component;

(2) examines the size, experience level, and geographic distribution of the operational personnel of the Department, including Customs and Border Protection officers, Border Patrol agents, Customs and Border Protection Air and Marine agents, Customs and Border Protection agriculture specialists, Federal Protective Service law enforcement security officers, Immigration and Customs Enforcement agents, Transportation Security Administration officers,
Federal air marshals, and members of the Coast
Guard; and

(3) makes recommendations for adjustments in
the management and administration of the Depart-
ment that would reduce deficiencies in the Depart-
ment’s capabilities, reduce costs, and enhance effi-
ciencies.

SEC. 1424. FIELD EFFICIENCIES PLAN.

(1) IN GENERAL.—Not later than 270 days
after the date of the enactment of this Act, the Sec-
retary of Homeland Security shall submit to the
Committee on Homeland Security of the House of
Representatives and Committee on Homeland Secu-
rity and Governmental Affairs of the Senate a field
efficiencies plan that—

(A) examines the facilities and administra-
tive and logistics functions of components of the
Department of Homeland Security located within
designated geographic areas; and

(B) provides specific recommendations and
an associated cost-benefit analysis for the con-
solidation of the facilities and administrative
and logistics functions of components of the De-
partment within each designated geographic
area.
(2) CONTENTS.—The field efficiencies plan submitted under paragraph (1) shall include the following:

(A) An accounting of leases held by the Department or its components that have expired in the current fiscal year or will be expiring in the next fiscal year, that have begun or been renewed in the current fiscal year, or that the Department or its components plan to sign or renew in the next fiscal year.

(B)(i) An evaluation for each designated geographic area of specific facilities at which components, or operational entities of components, of the Department may be closed or consolidated, including consideration of when leases expire or facilities owned by the Government become available.

(ii) The evaluation shall include consideration of potential consolidation with facilities of other Federal, State, or local entities, including—

(I) offices;

(II) warehouses;

(III) training centers;

(IV) housing;
(V) ports, shore facilities, and air-
fields;

(VI) laboratories; and

(VII) other assets as determined by
the Secretary.

(iii) The evaluation shall include the poten-
tial for the consolidation of administrative and
logistics functions, including—

(I) facility maintenance;

(II) fleet vehicle services;

(III) mail handling and shipping and
receiving;

(IV) facility security;

(V) procurement of goods and serv-
ices;

(VI) information technology and tele-
communications services and support; and

(VII) additional ways to improve unity
of effort and cost savings for field oper-
ations and related support activities as de-
termined by the Secretary.

(C) An implementation plan, including—

(i) near-term actions that can co-lo-
cate, consolidate, or dispose of property
within 24 months;
(ii) identifying long-term occupancy agreements or leases that cannot be changed without a significant cost to the Government; and

(iii) how the Department can ensure it has the capacity, in both personnel and funds, needed to cover up-front costs to achieve consolidation and efficiencies.

(D) An accounting of any consolidation in the Department or its component’s real estate footprint, including the co-location of personnel from different components, offices, and agencies within the Department.

SEC. 1425. RESOURCES TO RESPOND TO OPERATIONAL SURGES.

On an annual basis, the Secretary of Homeland Security shall provide to the Committee on Homeland Security of the House of Representatives and the Committee on Homeland Security and Governmental Affairs of the Senate information on the circumstances in which the Secretary exercised the authority during the preceding year to reprogram or transfer funds to address unforeseen costs, including the costs associated with operational surges, and information on any circumstances in which limitations on the transfer or reprogramming of funds im-
pacted the Secretary’s ability to address such unforeseen
costs.

SEC. 1426. DEPARTMENT OF HOMELAND SECURITY ROTA-
TION PROGRAM.

(a) ENHANCEMENTS TO THE ROTATION PROGRAM.—

Section 844(a) of the Homeland Security Act of 2002 (6
U.S.C. 414(a)) is amended as follows:

(1) In paragraph (1)—

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

(B) by striking “for employees of the De-
partment’’ and inserting “for certain personnel
within the Department’’.

(2) In paragraph (2)—

(A) by redesignating subparagraphs (A)
through (G) as subparagraphs (C) through (I),
and inserting before subparagraph (C), as so
redesignated, the following:

“(A) seek to foster greater Departmental
integration and unity of effort;

“(B) seek to help enhance the knowledge,
skills, and abilities of participating personnel
with respect to the Department’s programs,
policies, and activities;”;

•HR 6381 IH
(B) in subparagraph (D), as so redesignated, by striking "middle and senior level"; and

(C) in subparagraph (G), as so redesignated, by inserting before "invigorate" the following: "seek to improve morale and retention throughout the Department and".

(3) In paragraph (3)(B), by striking clause (iii) and redesignating clauses (iv) through (viii) as clauses (iii) through (vii).

(4) By redesignating paragraphs (4) and (5) as paragraphs (5) and (6), and inserting after paragraph (3) the following:

"(4) ADMINISTRATIVE MATTERS.—In carrying out any program established pursuant to this section, the Secretary shall—

"(A) before selecting employees for participation in such program, disseminate information broadly within the Department about the availability of the program, qualifications for participation in the program, including full-time employment within the employing component or office not less than one year, and the general provisions of the program;"
“(B) require each candidate for participation in the program to be nominated by the head of the candidate’s employing component or office and that the Secretary, or the Secretary’s designee, select each employee for the program solely on the basis of relative ability, knowledge, and skills, after fair and open competition that assures that all candidates receive equal opportunity;

“(C) ensure that each employee participating in the program shall be entitled to return, within a reasonable period of time after the end of the period of participation, to the position held by the employee, or a corresponding or higher position, in the employee’s employing component or office;

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

“(E) require that, during the period of participation by an employee in the program, performance evaluations for the employee—
“(i) shall be conducted by officials in the employee’s office or component with input from the supervisors of the employee at the component or office in which the employee is placed during that period; and
“(ii) shall be provided the same weight with respect to promotions and other rewards as performance evaluations for service in the employee’s office or component.”.

(b) Congressional Notification and Oversight.—Not later than 120 days after the date of the enactment of this Act, the Secretary of Homeland Security shall provide information to the Committee on Homeland Security of the House of Representatives and the Committee on Homeland Security and Governmental Affairs of the Senate about the status of the homeland security rotation program authorized by section 844 of the Homeland Security Act of 2002, as amended by this section.

Subtitle B—Department of Homeland Security Acquisition Accountability and Efficiency

SEC. 1431. DEFINITIONS.

(a) In General.—In this subtitle:
(1) Secretary.—The term “Secretary” means the Secretary of Homeland Security.

(2) Department.—The term “Department” means the Department of Homeland Security.

(3) Congressional Homeland Security Committees.—The term “congressional homeland security committees” means—

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

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

(b) Additional Definitions.—In this subtitle:

(1) Acquisition.—The term “acquisition” has the meaning provided in section 131 of title 41, United States Code.

(2) Best Practices.—The term “best practices”, with respect to acquisition, means a knowledge-based approach to capability development that includes identifying and validating needs; assessing alternatives to select the most appropriate solution; clearly establishing well-defined requirements; developing realistic cost assessments and schedules; se-
curing stable funding that matches resources to re-
quirements; demonstrating technology, design, and
manufacturing maturity; using milestones and exit
criteria or specific accomplishments that dem-
strate progress; adopting and executing standard-
ized processes with known success across programs;
establishing an adequate workforce that is qualified
and sufficient to perform necessary functions; and
integrating these capabilities into the Department’s
mission and business operations.

(c) AMENDMENTS TO DEFINITIONS IN HOMELAND
SECURITY ACT OF 2002.—Section 2 of the Homeland Secu-
ry Act of 2002 is amended—

(1) by striking “In this Act,” and inserting “(a)
IN GENERAL.—In this Act,”;

(2) in paragraph (2)—

(A) by inserting “(A)” after “(2)”; and

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

“(B) The term ‘congressional homeland security
committees’ means—

“(i) the Committee on Homeland Security
of the House of Representatives and the Com-
mittee on Homeland Security and Government-
mental Affairs of the Senate; and
“(ii) the Committees on Appropriations of
the House of Representatives and of the Sen-
ate, where appropriate.”; and
(3) by adding at the end the following new sub-
section:
“(b) ACQUISITION-RELATED DEFINITIONS.—In this
Act, the following definitions apply:
“(1) ACQUISITION.—The term ‘acquisition’ has
the meaning provided in section 131 of title 41,
United States Code.
“(2) ACQUISITION DECISION AUTHORITY.—The
term ‘acquisition decision authority’ means the au-
thority, held by the Secretary acting through the
Deputy Secretary or Under Secretary for Manage-
ment—
“(A) to ensure compliance with Federal
law, the Federal Acquisition Regulation, and
Department acquisition management directives;
“(B) to review (including approving, halting,
modifying, or cancelling) an acquisition
program through the life cycle of the program;
“(C) to ensure that program managers
have the resources necessary to successfully
execute an approved acquisition program;
“(D) to ensure good program management of cost, schedule, risk, and system performance of the acquisition, including assessing acquisition program baseline breaches and directing any corrective action for such breaches; and

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

“(3) ACQUISITION DECISION EVENT.—The term ‘acquisition decision event’, with respect to an investment or acquisition program, means a predeter-mined point within the acquisition phases of the investment or acquisition program at which the investment or acquisition program will undergo a review prior to commencement of the next phase.

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

“(5) Acquisition Program Baseline.—The term ‘acquisition program baseline’, with respect to an acquisition program, means a summary of the cost, schedule, and performance parameters, expressed in standard, measurable, quantitative terms, which must be met in order to accomplish the goals of the program.

“(6) Capability Development Plan.—The term ‘capability development plan’, with respect to a proposed acquisition, means the document that the Acquisition Review Board approves for the first acquisition decision event related to validating the need of a proposed acquisition.

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

“(8) LIFE CYCLE COST.—The term ‘life cycle cost’, with respect to an acquisition program, means all costs associated with research, development, procurement, operation, integrated logistics support, and disposal under the program, including supporting infrastructure that plans, manages, and executes the program over its full life, and costs of common support items incurred as a result of the program.

“(9) MAJOR ACQUISITION PROGRAM.—The term ‘major acquisition program’ means a Department acquisition program that is estimated by the Secretary to require an eventual total expenditure of at least $300,000,000 (based on fiscal year 2015 constant dollars) over its life cycle cost.”.

PART 1—ACQUISITION AUTHORITIES

SEC. 1441. ACQUISITION AUTHORITIES FOR UNDER SECRETARY FOR MANAGEMENT.

Section 701 of the Homeland Security Act of 2002 (6 U.S.C. 341), as amended by section 1417 of this title, is further amended by adding at the end the following:
“(e) Acquisition and Related Responsibilities.—

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

“(2) duties and responsibilities.—In addition to the authority and functions specified in section 1702(b) of title 41, United States Code, the duties and responsibilities of the Under Secretary for Management related to acquisition include the following:

“(A) Advising the Secretary regarding acquisition management activities, taking into account risks of failure to achieve cost, schedule, or performance parameters, to ensure that the Department achieves its mission through the adoption of widely accepted program management best practices and standards.
“(B) Exercising the acquisition decision authority to approve, halt, modify (including the rescission of approvals of program milestones), or cancel major acquisition programs, unless the Under Secretary delegates the authority to a Component Acquisition Executive pursuant to paragraph (3).

“(C) Establishing policies for acquisition that implement an approach that takes into account risks of failure to achieve cost, schedule, or performance parameters that all components of the Department shall comply with, including outlining relevant authorities for program managers to effectively manage acquisition programs.

“(D) Ensuring that each major acquisition program has a Department-approved acquisition program baseline, pursuant to the Department’s acquisition management policy.

“(E) Ensuring that the heads of components and Component Acquisition Executives comply with Federal law, the Federal Acquisition Regulation, and Department acquisition management directives.
“(F) Ensuring that grants and financial assistance are provided only to individuals and organizations that are not suspended or debarred.

“(G) Distributing guidance throughout the Department to ensure that contractors involved in acquisitions, particularly companies that access the Department’s information systems and technologies, adhere to internal cybersecurity policies established by the Department of Homeland Security.

“(3) DELEGATION OF ACQUISITION DECISION AUTHORITY.—

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

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

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

“(ii) The Component Acquisition Executive has adequate, experienced, dedicated program management professional staff commensurate with the size of the delegated portfolio.

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

“(4) EXCLUDED PARTIES LIST SYSTEM CONSULTATION.—The Under Secretary for Management shall require that all Department contracting and procurement officials consult the Excluded Parties List System (or successor system) as maintained by the General Services Administration prior to awarding a contract or grant or entering into other transactions to ascertain whether the selected contractor
is excluded from receiving Federal contracts, certain subcontracts, and certain types of Federal financial and nonfinancial assistance and benefits.

“(5) Relationship to Under Secretary for Science and Technology.—

“(A) In general.—Nothing in this subsection shall diminish the authority granted to the Under Secretary for Science and Technology under this Act. The Under Secretary for Management and the Under Secretary for Science and Technology shall cooperate in matters related to the coordination of acquisitions across the Department so that investments of the Directorate of Science and Technology can support current and future requirements of the components.

“(B) Operational testing and evaluation.—The Under Secretary for Science and Technology shall—

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

“(I) complete operational testing and evaluation of technologies and systems;
“(II) use independent verification and validation of operational test and evaluation implementation and results; and

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

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

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

SEC. 1442. ACQUISITION AUTHORITIES FOR CHIEF FINANCIAL OFFICER.

Section 702 of the Homeland Security Act of 2002 (6 U.S.C. 342), as amended by section 1618 of this title, is further amended by adding at the end of subsection (c)(2) the following new subparagraph:
“(J) Notwithstanding section 902 of title 31, United States Code, provide leadership over financial management policy and programs for the Department as they relate to the Department’s acquisitions programs, in consultation with the Under Secretary for Management.”

SEC. 1443. ACQUISITION AUTHORITIES FOR CHIEF INFORMATION OFFICER.

Section 703 of the Homeland Security Act of 2002 (6 U.S.C. 343), as amended by section 1620(a) of this title, is further amended by adding at the end the following new subsection:

“(f) Acquisition Responsibilities.—Notwithstanding section 11315 of title 40, United States Code, the acquisition responsibilities of the Chief Information Officer, in consultation with the Under Secretary for Management, shall include the following:

“(1) Oversee the management of the Homeland Security Enterprise Architecture and ensure that, before each acquisition decision event, approved information technology acquisitions comply with departmental information technology management processes, technical requirements, and the Homeland Security Enterprise Architecture, and in any case in which information technology acquisitions do not
comply with the Department’s management directives, make recommendations to the Acquisition Review Board regarding such noncompliance.

“(2) Be responsible for providing recommendations to the Acquisition Review Board established in section 836 of this Act on information technology programs, and be responsible for developing information technology acquisition strategic guidance.”.

SEC. 1444. REQUIREMENTS TO ENSURE GREATER ACCOUNTABILITY FOR ACQUISITION PROGRAMS.

(a) IN GENERAL.—Title VII of the Homeland Security Act of 2002 (6 U.S.C. 341 et seq.), as amended by sections 1419(a) and 1422(a) of this title, is further amended by adding at the end the following:

“SEC. 710. REQUIREMENTS TO ENSURE GREATER ACCOUNTABILITY FOR ACQUISITION PROGRAMS.

“(a) Requirement To Establish Mechanism.—Within the Management Directorate, the Under Secretary for Management shall establish a mechanism to prioritize improving the accountability, standardization, and transparency of major acquisition programs of the Department in order to increase opportunities for effectiveness and ef-
ficiencies and to serve as the central oversight function of all Department acquisition programs.

“(b) Responsibilities of Executive Director.—The Under Secretary for Management shall designate an Executive Director to oversee the requirement under subsection (a). The Executive Director shall report directly to the Under Secretary and shall carry out the following responsibilities:

“(1) Monitor the performance of Department acquisition programs regularly between acquisition decision events to identify problems with cost, performance, or schedule that components may need to address to prevent cost overruns, performance issues, or schedule delays.

“(2) Assist the Under Secretary for Management in managing the Department’s acquisition portfolio.

“(3) Conduct oversight of individual acquisition programs to implement Department acquisition program policy, procedures, and guidance with a priority on ensuring the data it collects and maintains from its components is accurate and reliable.

“(4) Serve as the focal point and coordinator for the acquisition life cycle review process and as
the executive secretariat for the Acquisition Review Board established under section 836 of this Act.

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

“(6) Engage in the strategic planning and performance evaluation process required under section 306 of title 5, United States Code, and sections 1105(a)(28), 1115, 1116, and 9703 of title 31, United States Code, by supporting the Chief Procurement Officer in developing strategies and specific plans for hiring, training, and professional development in order to rectify any deficiency within the Department’s acquisition workforce.

“(7) Oversee the Component Acquisition Executive structure to ensure it has sufficient capabilities and complies with Department policies.

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

“(9) In the event that a program manager’s certification or actions need review for purposes of
promotion or removal, provide input, in consultation with the relevant Component Acquisition Executive, into the relevant program manager’s performance evaluation, and report positive or negative experiences to the relevant certifying authority.

“(10) Provide technical support and assistance to Department acquisitions and acquisition personnel in conjunction with the Chief Procurement Officer.

“(11) Prepare the Department’s Comprehensive Acquisition Status Report, as required by the Department of Homeland Security Appropriations Act, 2013 (division D of Public Law 113–6; 127 Stat. 343) and section 840 of this Act, and make such report available to congressional homeland security committees.

“(12) Prepare the Department’s Quarterly Program Accountability Report as required by section 840 of this Act, and make such report available to the congressional homeland security committees.

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

“(1) define baseline requirements and document
changes to those requirements, as appropriate;

“(2) establish a complete life cycle cost estimate
with supporting documentation, including an acquisi-
tion program baseline;

“(3) verify each life cycle cost estimate against
independent cost estimates, and reconcile any dif-
fferences;

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

“(5) develop and maintain a schedule that is
consistent with scheduling best practices as identi-
fied by the Comptroller General of the United
States, including, in appropriate cases, an integrated
master schedule; and

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

“SEC. 711. ACQUISITION DOCUMENTATION.

“(a) In General.—For each major acquisition pro-
gram, the Executive Director responsible for the prepara-
tion of the Comprehensive Acquisition Status Report, pur-
suant to paragraph (11) of section 710(b), shall require
certain acquisition documentation to be submitted by Department components or offices.

“(b) WAIVER.—The Secretary may waive the requirement for submission under subsection (a) for a program for a fiscal year if either—

“(1) the program has not—

“(A) entered the full rate production phase in the acquisition life cycle;

“(B) had a reasonable cost estimate established; and

“(C) had a system configuration defined fully; or

“(2) the program does not meet the definition of ‘capital asset’, as defined by the Director of the Office of Management and Budget.

“(c) CONGRESSIONAL OVERSIGHT.—At the same time the President’s budget is submitted for a fiscal year under section 1105(a) of title 31, United States Code, the Secretary shall submit to the Committee on Homeland Security of the House of Representatives and Committee on Homeland Security and Governmental Affairs of the Senate information on the exercise of authority under subsection (b) in the prior fiscal year that includes the following specific information regarding each program for which a waiver is issued under subsection (b):
“(1) The grounds for granting a waiver for that program.

“(2) The projected cost of that program.

“(3) The proportion of a component’s annual acquisition budget attributed to that program, as available.

“(4) Information on the significance of the program with respect to the component’s operations and execution of its mission.”.

(b) CLERICAL AMENDMENT.—The table of contents in section 1(b) of the Homeland Security Act of 2002 (6 U.S.C. 101 et seq.) is further amended by adding after the item relating to section 1419 the following new item:

“Sec. 710. Requirements to ensure greater accountability for acquisition programs.

“Sec. 711. Acquisition documentation.”.

PART 2—ACQUISITION PROGRAM MANAGEMENT

DISCIPLINE

SEC. 1451. ACQUISITION REVIEW BOARD.

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

“SEC. 836. ACQUISITION REVIEW BOARD.

“(a) IN GENERAL.—The Secretary shall establish an Acquisition Review Board (in this section referred to as the ‘Board’) to strengthen accountability and uniformity within the Department acquisition review process, review
major acquisition programs, and review the use of best practices.

“(b) COMPOSITION.—The Deputy Secretary or Under Secretary for Management shall serve as chair of the Board. The Secretary shall also ensure participation by other relevant Department officials, including at least 2 component heads or their designees, as permanent members of the Board.

“(c) MEETINGS.—The Board shall meet every time a major acquisition program needs authorization to proceed from acquisition decision events through the acquisition life cycle and to consider any major acquisition program in breach as necessary. The Board may also be convened for non-major acquisitions that are deemed high-risk by the Executive Director referred to in section 710(b) of this Act. The Board shall also meet regularly for purposes of ensuring all acquisitions processes proceed in a timely fashion to achieve mission readiness.

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

“(1) Determine whether a proposed acquisition has met the requirements of key phases of the acquisition life cycle framework and is able to proceed to the next phase and eventual full production and deployment.
“(2) Oversee executable business strategy, resources, management, accountability, and alignment to strategic initiatives.

“(3) Support the person with acquisition decision authority for an acquisition in determining the appropriate direction for the acquisition at key acquisition decision events.

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

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

“(6) Ensure that practices are adopted and implemented to require consideration of trade-offs among cost, schedule, and performance objectives as part of the process for developing requirements for major acquisition programs prior to the initiation of the second acquisition decision event, including, at a minimum, the following practices:
“(A) Department officials responsible for acquisition, budget, and cost estimating functions are provided with the appropriate opportunity to develop estimates and raise cost and schedule matters before performance objectives are established for capabilities when feasible.

“(B) Full consideration of possible trade-offs among cost, schedule, and performance objectives for each alternative is considered.

“(e) Acquisition Program Baseline Report Requirement.—If the person exercising acquisition decision authority over a major acquisition program approves the program to proceed into the planning phase before it has a Department-approved acquisition program baseline, then the Under Secretary for Management shall create and approve an acquisition program baseline report on the decision, and the Secretary shall—

“(1) within 7 days after an acquisition decision memorandum is signed, notify in writing the congressional homeland security committees of such decision; and

“(2) within 60 days after the acquisition decision memorandum is signed, submit a report to such committees stating the rationale for the decision and
a plan of action to require an acquisition program
baseline for the program.

“(f) Best Practices Defined.—In this section, the term ‘best practices’ has the meaning provided in section 4(b) of the DHS Headquarters Reform and Improvement Act of 2015.”.

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

“Sec. 836. Acquisition Review Board.”.

SEC. 1452. REQUIREMENTS TO REDUCE DUPLICATION IN ACQUISITION PROGRAMS.

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

“SEC. 837. REQUIREMENTS TO REDUCE DUPLICATION IN ACQUISITION PROGRAMS.

“(a) Requirement To Establish Policies.—In an effort to reduce unnecessary duplication and inefficiency for all Department investments, including major acquisition programs, the Deputy Secretary, in consultation with the Under Secretary for Management, shall establish Department-wide policies to integrate all phases of the investment life cycle and help the Department identify, vali-
date, and prioritize common component requirements for major acquisition programs in order to increase opportunities for effectiveness and efficiencies. The policies shall also include strategic alternatives for developing and facilitating a Department component-driven requirements process that includes oversight of a development test and evaluation capability; identification of priority gaps and overlaps in Department capability needs; and provision of feasible technical alternatives, including innovative commercially available alternatives, to meet capability needs.

“(b) MECHANISMS TO CARRY OUT REQUIREMENT.—

The Under Secretary for Management shall coordinate the actions necessary to carry out subsection (a), using such mechanisms as considered necessary by the Secretary to help the Department reduce unnecessary duplication and inefficiency for all Department investments, including major acquisition programs.

“(c) COORDINATION.—In coordinating the actions necessary to carry out subsection (a), the Deputy Secretary shall consult with the Under Secretary for Management, Component Acquisition Executives, and any other Department officials, including the Under Secretary for Science and Technology or his designee, with specific knowledge of Department or component acquisition capa-
bilities to prevent unnecessary duplication of require-
ments.

“(d) ADVISORS.—The Deputy Secretary, in consulta-
tion with the Under Secretary for Management, shall seek
and consider input within legal and ethical boundaries
from members of Federal, State, local, and tribal govern-
ments, nonprofit organizations, and the private sector, as
appropriate, on matters within their authority and exper-
tise in carrying out the Department’s mission.

“(e) MEETINGS.—The Deputy Secretary, in consulta-
tion with the Under Secretary for Management, shall meet
at least quarterly and communicate with components often
to ensure that components do not overlap or duplicate
spending or activities on major investments and acquisi-
tion programs within their areas of responsibility.

“(f) RESPONSIBILITIES.—In carrying out this sec-
tion, the responsibilities of the Deputy Secretary, in con-
sultation with the Under Secretary for Management, are
as follows:

“(1) To review and validate the requirements
documents of major investments and acquisition pro-
cgrams prior to acquisition decision events of the in-
vestments or programs.

“(2) To ensure the requirements and scope of
a major investment or acquisition program are sta-
ble, measurable, achievable, at an acceptable risk
level, and match the resources planned to be avail-
able.

“(3) Before any entity of the Department
issues a solicitation for a new contract, coordinate
with other Department entities as appropriate to
prevent unnecessary duplication and inefficiency
and—

“(A) to implement portfolio reviews to
identify common mission requirements and
crosscutting opportunities among components
to harmonize investments and requirements and
prevent unnecessary overlap and duplication
among components; and

“(B) to the extent practicable, to stand-
ardize equipment purchases, streamline the ac-
quision process, improve efficiencies, and con-
duct best practices for strategic sourcing.

“(4) To ensure program managers of major in-
vestments and acquisition programs conduct anal-
yses, giving particular attention to factors such as
cost, schedule, risk, performance, and operational ef-
ficiency in order to determine that programs work as
intended within cost and budget expectations.
“(5) To propose schedules for delivery of the operational capability needed to meet each Department investment and major acquisition program.

“(g) BEST PRACTICES DEFINED.—In this section, the term ‘best practices’ has the meaning provided in section 4(b) of the DHS Headquarters Reform and Improvement Act of 2015.”.

(b) CLERICAL AMENDMENT.—The table of contents in section 1(b) of the Homeland Security Act of 2002 (6 U.S.C. 101 et seq.) is further amended by adding after the item relating to section 836 the following new item:

“Sec. 837. Requirements to reduce duplication in acquisition programs.”.

SEC. 1453. GOVERNMENT ACCOUNTABILITY OFFICE REVIEW OF BOARD AND OF REQUIREMENTS TO REDUCE DUPLICATION IN ACQUISITION PROGRAMS.

(a) REVIEW REQUIRED.—The Comptroller General of the United States shall conduct a review of the effectiveness of the Acquisition Review Board established under section 836 of the Homeland Security Act of 2002 (as added by section 1451) and the requirements to reduce unnecessary duplication in acquisition programs established under section 837 of such Act (as added by section 1452) in improving the Department’s acquisition management process.
(b) Scope of Report.—The review shall include the following:

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

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

(3) A statement of how regularly each major acquisition program is reviewed by the Board, how often the Board stops major acquisition programs from moving forward in the phases of the acquisition life cycle process, and the number of major acquisition programs that have been halted because of problems with operational effectiveness, schedule delays, or cost overruns.

(4) An assessment of the effectiveness of the Board in impacting acquisition decisionmaking within the Department, including the degree to which the Board impacts decisionmaking within other headquarters mechanisms and bodies involved in the administration of acquisition activities.
(c) **Report Required.**—The Comptroller General shall submit to the congressional homeland security committees a report on the review required by this section not later than 1 year after the date of the enactment of this Act. The report shall be submitted in unclassified form but may include a classified annex.

**SEC. 1454. EXCLUDED PARTY LIST SYSTEM WAIVERS.**

The Secretary of Homeland Security shall provide notification to the congressional homeland security committees within 5 days after the issuance of a waiver by the Secretary of Federal requirements that an agency not engage in business with a contractor in the Excluded Party List System (or successor system) as maintained by the General Services Administration and an explanation for a finding by the Secretary that a compelling reason exists for this action.

**SEC. 1455. INSPECTOR GENERAL OVERSIGHT OF SUSPENSION AND DEBARMENT.**

The Inspector General of the Department of Homeland Security—

(1) may audit decisions about grant and procurement awards to identify instances where a contract or grant was improperly awarded to a suspended or debarred entity and whether corrective actions were taken to prevent recurrence; and
(2) shall review the suspension and debarment program throughout the Department of Homeland Security to assess whether suspension and debarment criteria are consistently applied throughout the Department and whether disparities exist in the application of such criteria, particularly with respect to business size and categories.

PART 3—ACQUISITION PROGRAM MANAGEMENT

ACCOUNTABILITY AND TRANSPARENCY

SEC. 1461. CONGRESSIONAL NOTIFICATION AND OTHER REQUIREMENTS FOR MAJOR ACQUISITION PROGRAM BREACH.

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

“SEC. 838. CONGRESSIONAL NOTIFICATION AND OTHER REQUIREMENTS FOR MAJOR ACQUISITION PROGRAM BREACH.

“(a) BREACH DEFINED.—The term ‘breach’, with respect to a major acquisition program, means a failure to meet any cost, schedule, or performance parameter specified in the acquisition program baseline.

“(b) REQUIREMENTS WITHIN DEPARTMENT IF BREACH OCCURS.—
“(1) Notifications.—

“(A) Notification of breach.—If a breach occurs in a major acquisition program, the program manager for that program shall notify the Component Acquisition Executive for the program, the head of the component concerned, the Executive Director referred to in section 710(b) of this Act, the Under Secretary for Management, and the Deputy Secretary.

“(B) Notification to Secretary.—If a major acquisition program has a breach with a cost overrun greater than 15 percent or a schedule delay greater than 180 days from the costs or schedule set forth in the acquisition program baseline for the program, the Secretary and the Inspector General of the Department shall be notified not later than 5 business days after the breach is identified.

“(2) Remediation plan and root cause analysis.—

“(A) In general.—In the case of a breach with a cost overrun greater than 15 percent or a schedule delay greater than 180 days from the costs or schedule set forth in the acquisition program baseline, a remediation plan
and root cause analysis is required, and the
Under Secretary for Management or his des-
ignee shall establish a date for submission with-
in the Department of a breach remediation plan
and root cause analysis in accordance with this
subsection.

“(B) Remedia**tion Plan.—The remedia-
tion plan required under this subsection shall
be submitted in writing to the head of the com-
ponent concerned, the Executive Director re-
ferred to in section 710(b) of this Act, and the
Under Secretary for Management. The plan
shall—

“(i) explain the circumstances of the
breach;

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

“(iii) propose corrective action to con-
trol cost growth, schedule delays, or per-
formance issues;

“(iv) in coordination with Component
Acquisition Executive, discuss all options
considered, including the estimated impact
on cost, schedule, or performance of the
program if no changes are made to current
requirements, the estimated cost of the
program if requirements are modified, and
the extent to which funding from other
programs will need to be reduced to cover
the cost growth of the program; and

“(v) explain the rationale for why the
proposed corrective action is recommended.

“(C) Root cause analysis.—The root
cause analysis required under this subsection
shall determine the underlying cause or causes
of shortcomings in cost, schedule, or perform-
ance of the program, including the role, if any,
of the following:

“(i) Unrealistic performance expecta-
tions.

“(ii) Unrealistic baseline estimates for
cost or schedule or changes in program re-
quirements.

“(iii) Immature technologies or exces-
sive manufacturing or integration risk.

“(iv) Unanticipated design, engineer-
ing, manufacturing, or technology integra-
tion issues arising during program per-
formance.
“(v) Changes in procurement quantities.

“(vi) Inadequate program funding or changes in planned out-year funding from one 5-year funding plan to the next 5-year funding plan as outlined in the Future Years Homeland Security Program required under section 874 of this Act.

“(vii) Legislative, legal, or regulatory changes.

“(viii) Inadequate program management personnel, including lack of training, credentials, certifications, or use of best practices.

“(3) CORRECTION OF BREACH.—The Under Secretary for Management or his designee shall establish a date for submission within the Department of a program of corrective action that ensures that one of the following actions has occurred:

“(A) The breach has been corrected and the program is again in compliance with the original acquisition program baseline parameters.

“(B) A revised acquisition program baseline has been approved.
“(C) The program has been halted or can-
celled.
“(c) REQUIREMENTS RELATING TO CONGRESSIONAL
NOTIFICATION IF BREACH OCCURS.—
“(1) NOTIFICATION TO CONGRESS.—If a notifi-
cation is made under subsection (b)(1)(B) for a
breach in a major acquisition program with a cost
overrun greater than 15 percent or a schedule delay
greater than 180 days from the costs or schedule set
forth in the acquisition program baseline, or with an
anticipated failure for any key performance thresh-
old or parameter specified in the acquisition pro-
gram baseline, the Under Secretary for Management
shall notify the congressional homeland security
committees of the breach in the next quarterly Com-
prehensive Acquisition Status Report after the
Under Secretary for Management receives the notifi-
cation from the program manager under subsection
(b)(1)(B).
“(2) SUBSTANTIAL VARIANCES IN COSTS OR
SCHEDULE.—If a likely cost overrun is greater than
20 percent or a likely delay is greater than 12
months from the costs and schedule set forth in the
acquisition program baseline for a major acquisition
program, the Under Secretary for Management shall
include in the notification required in (c)(1) a written certification, with supporting explanation, that—

“(A) the acquisition is essential to the accomplishment of the Department’s mission;

“(B) there are no alternatives to such capability or asset that will provide equal or greater capability in both a more cost-effective and timely manner;

“(C) the new acquisition schedule and estimates for total acquisition cost are reasonable; and

“(D) the management structure for the acquisition program is adequate to manage and control performance, cost, and schedule.

“(3) Submissions to Congress.—Not later than 30 calendar days after submission to such committees of a breach notification under paragraph (1) of this section for a major acquisition program, the Under Secretary for Management shall submit to such committees the following:

“(A) A copy of the remediation plan and the root cause analysis prepared under subsection (b)(2) for the program.

“(B) A statement describing the corrective action or actions that have occurred pursuant
to subsection (b)(3) for the program, with a justification for the action or actions.

“(d) ADDITIONAL ACTIONS IF BREACH OCCURS.—

“(1) PROHIBITION ON OBLIGATION OF FUNDS.—During the 90-day period following submission under subsection (c)(3) of a remediation plan, root cause analysis, and statement of corrective actions with respect to a major acquisition program, the Under Secretary for Management shall submit a certification described in paragraph (2) of this subsection to the congressional homeland security committees. If the Under Secretary for Management does not submit such certification by the end of such 90-day period, then funds appropriated to the major acquisition program shall not be obligated until the Under Secretary for Management submits such certification.

“(2) CERTIFICATION.—For purposes of paragraph (1), the certification described in this paragraph is a certification that—

“(A) the Department has adjusted or restructured the program in a manner that addresses the root cause or causes of the cost growth in the program; and
“(B) the Department has conducted a thorough review of the breached program’s acquisition decision event approvals and the current acquisition decision event approval for the breached program has been adjusted as necessary to account for the restructured program.”.

(b) CLERICAL AMENDMENT.—The table of contents in section 1(b) of the Homeland Security Act of 2002 (6 U.S.C. 101 et seq.) is further amended by adding after the item relating to section 837 the following new item:

“Sec. 838. Congressional notification and other requirements for major acquisition program breach.”.

SEC. 1462. MULTIYEAR ACQUISITION STRATEGY.

(a) IN GENERAL.—

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

“SEC. 839. MULTIYEAR ACQUISITION STRATEGY.

“(a) MULTIYEAR ACQUISITION STRATEGY REQUIRED.—Not later than 1 year after the date of the enactment of this section, the Secretary shall submit to the appropriate homeland security committees a multiyear acquisition strategy to guide the overall direction of the acquisitions of the Department while allowing flexibility to
deal with ever-changing threats and risks and to help in-
dustry better understand, plan, and align resources to
meet the future acquisition needs of the Department. The
strategy shall be updated and included in each Future
Years Homeland Security Program required under section
874 of this Act.

“(b) CONSULTATION.—In developing the strategy,
the Secretary shall consult with others as the Secretary
deems appropriate, including headquarters, components,
employees in the field, and when appropriate, individuals
from industry and the academic community.

“(c) FORM OF STRATEGY.—The report shall be sub-
mitted in unclassified form but may include a classified
annex for any sensitive or classified information if nec-
essary. The Department also shall publish the plan in an
unclassified format that is publicly available.

“(d) CONTENTS OF STRATEGY.—The strategy shall
include the following:

“(1) PRIORITIZED LIST.—A systematic and in-
tegrated prioritized list developed by the Under Sec-
retary for Management or his designee in coordina-
tion with all of the Component Acquisition Execu-
tives of Department major acquisition programs that
Department and component acquisition investments
seek to address, that includes the expected security
and economic benefit of the program or system and
an analysis of how the security and economic benefit
derived from the program or system will be meas-
ured.

“(2) INVENTORY.—A plan to develop a reliable
Department-wide inventory of investments and real
property assets to help the Department plan, budg-
et, schedule, and acquire upgrades of its systems
and equipment and plan for the acquisition and
management of future systems and equipment.

“(3) FUNDING GAPS.—A plan to address fund-
ing gaps between funding requirements for major ac-
quision programs and known available resources in-
cluding, to the maximum extent practicable, ways of
leveraging best practices to identify and eliminate
overpayment for items to prevent wasteful pur-
chasing, achieve the greatest level of efficiency and
cost savings by rationalizing purchases, aligning
pricing for similar items, and utilizing purchase tim-
ing and economies of scale.

“(4) IDENTIFICATION OF CAPABILITIES.—An
identification of test, evaluation, modeling, and sim-
ulation capabilities that will be required to support
the acquisition of the technologies to meet the needs
of the plan and ways to leverage to the greatest ex-
tent possible the emerging technology trends and re-
search and development trends within the public and
private sectors and an identification of ways to en-
sure that the appropriate technology is acquired and
integrated into the Department’s operating doctrine
and procured in ways that improve mission perform-
ance.

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

“(6) FOCUS ON INCENTIVES TO SAVE TAX-
pAYER DOLLARS.—An assessment of ways the De-
partment can develop incentives for program man-
agers and senior Department acquisition officials to
prevent cost overruns, avoid schedule delays, and
achieve cost savings in major acquisition programs.

“(7) FOCUS ON ADDRESSING DELAYS AND BID
PROTESTS.—An assessment of ways the Department
can improve the acquisition process to minimize cost
overruns in requirements development, procurement
announcements, requests for proposals, evaluation of proposals, protests of decisions and awards and through the use of best practices as defined in section 4(b) of the DHS Headquarters Reform and Improvement Act of 2015 and lessons learned by the Department and other Federal agencies.

“(8) FOCUS ON IMPROVING OUTREACH.—An identification and assessment of ways to increase opportunities for communication and collaboration with industry, small and disadvantaged businesses, intragovernment entities, university centers of excellence, accredited certification and standards development organizations, and national laboratories to ensure that the Department understands the market for technologies, products, and innovation that is available to meet its mission needs to inform the requirements-setting process and before engaging in an acquisition, including—

“(A) methods designed especially to engage small and disadvantaged businesses and a cost-benefit analysis of the tradeoffs that small and disadvantaged businesses provide, barriers to entry for small and disadvantaged businesses, and unique requirements for small and disadvantaged businesses; and
“(B) within the Department Vendor Communication Plan and Market Research Guide, instructions for interaction by program managers with such entities to prevent misinterpretation of acquisition regulations and to permit freedom within legal and ethical boundaries for program managers to interact with such businesses with transparency.

“(9) COMPETITION.—A plan regarding competition as described in subsection (e).

“(10) ACQUISITION WORKFORCE.—A plan regarding the Department acquisition workforce as described in subsection (f).

“(11) FEASIBILITY OF WORKFORCE DEVELOPMENT FUND PILOT PROGRAM.—An assessment of the feasibility of conducting a pilot program to establish an acquisition workforce development fund as described in subsection (g).

“(e) COMPETITION PLAN.—The strategy shall also include a plan (referred to in subsection (d)(9)) that shall address actions to ensure competition, or the option of competition, for major acquisition programs. The plan may include assessments of the following measures in appropriate cases if such measures are cost effective:

“(1) Competitive prototyping.
“(2) Dual-sourcing.
“(3) Unbundling of contracts.
“(4) Funding of next-generation prototype systems or subsystems.
“(5) Use of modular, open architectures to enable competition for upgrades.
“(6) Acquisition of complete technical data packages.
“(7) Periodic competitions for subsystem upgrades.
“(8) Licensing of additional suppliers, including small businesses.
“(9) Periodic system or program reviews to address long-term competitive effects of program decisions.
“(f) ACQUISITION WORKFORCE PLAN.—
“(1) ACQUISITION WORKFORCE.—The strategy shall also include a plan (referred to in subsection (d)(10)) to address Department acquisition workforce accountability and talent management that identifies the acquisition workforce needs of each component performing acquisition functions and develops options for filling those needs with qualified individuals, including a cost-benefit analysis of contracting for acquisition assistance.
“(2) ADDITIONAL MATTERS COVERED.—The acquisition workforce plan shall address ways to—

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

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

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

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

“(E) designate the acquisition positions that will be necessary to support the Depart-
ment acquisition requirements, including in the fields of—

“(i) program management;
“(ii) systems engineering;
“(iii) procurement, including contracting;
“(iv) test and evaluation;
“(v) life cycle logistics;
“(vi) cost estimating and program financial management; and
“(vii) additional disciplines appropriate to Department mission needs;
“(F) strengthen the performance of contracting officer’s representatives (as defined in subpart 1.602–2 and subpart 2.101 of the Federal Acquisition Regulation), including by—
“(i) assessing the extent to which contracting officer’s representatives are certified and receive training that is appropriate;
“(ii) determining what training is most effective with respect to the type and complexity of assignment; and
“(iii) implementing actions to improve training based on such assessment; and
“(G) identify ways to increase training for relevant investigators and auditors to examine fraud in major acquisition programs, including identifying opportunities to leverage existing Government and private sector resources in co-ordination with the Inspector General of the Department.

“(g) FEASIBILITY OF WORKFORCE DEVELOPMENT FUND PILOT PROGRAM.—The strategy shall also include an assessment (referred to in subsection (d)(11)) of the feasibility of conducting a pilot program to establish a Homeland Security Acquisition Workforce Development Fund (in this subsection referred to as the ‘Fund’) to ensure the Department acquisition workforce has the capacity, in both personnel and skills, needed to properly perform its mission and ensure that the Department receives the best value for the expenditure of public resources. The assessment shall address the following:

“(1) Ways to fund the Fund, including the use of direct appropriations, or the credit, transfer, or deposit of unobligated or unused funds from Department components into the Fund to remain available for obligation in the fiscal year for which credited, transferred, or deposited and to remain available for successive fiscal years.
“(2) Ways to reward the Department acquisition workforce and program managers for good program management in controlling cost growth, limiting schedule delays, and ensuring operational effectiveness through providing a percentage of the savings or general acquisition bonuses.

“(3) Guidance for the administration of the Fund that includes provisions to do the following:

“(A) Describe the costs and benefits associated with the use of direct appropriations or credit, transfer, or deposit of unobligated or unused funds to finance the Fund.

“(B) Describe the manner and timing for applications for amounts in the Fund to be submitted.

“(C) Explain the evaluation criteria to be used for approving or prioritizing applications for amounts in the Fund in any fiscal year.

“(D) Explain the mechanism to report to Congress on the implementation of the Fund on an ongoing basis.

“(E) Detail measurable performance metrics to determine if the Fund is meeting the objective to improve the acquisition workforce
and to achieve cost savings in acquisition man-
agement.”.

(2) CLERICAL AMENDMENT.—The table of con-
tents in section 1(b) of the Homeland Security Act
of 2002 (6 U.S.C. 101 et seq.) is further amended
by adding after the item relating to section 838 the
following new item:

“Sec. 839. Multiyear acquisition strategy.”.

(b) CONFORMING AMENDMENT TO FUTURE YEARS
HOMELAND SECURITY PROGRAM.—Section 874(b) of the
Homeland Security Act of 2002 (6 U.S.C. 454(b)) is
amended—

(1) by striking “and” at the end of paragraph
(2);

(2) by striking the period at the end of para-
graph (3) and inserting “; and”; and

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

“(4) include the multiyear acquisition strategy
required under section 839 of this Act.”.

SEC. 1463. ACQUISITION REPORTS.
(a) IN GENERAL.—Subtitle D of title VIII of the
is further amended by adding at the end the following new
section:
“SEC. 840. ACQUISITION REPORTS.

“(a) COMPREHENSIVE ACQUISITION STATUS REPORT.—

“(1) IN GENERAL.—The Under Secretary for Management each year shall submit to the congressional homeland security committees, at the same time as the President’s budget is submitted for a fiscal year under section 1105(a) of title 31, United States Code, a comprehensive acquisition status report. The report shall include the following:

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

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

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

“(2) INFORMATION FOR MAJOR ACQUISITION
PROGRAMS.—For each major acquisition program,
the report shall include the following:

“(A) A narrative description, including
current gaps and shortfalls, the capabilities to
be fielded, and the number of planned incre-
ments or units.

“(B) Acquisition Review Board (or other
board designated to review the acquisition) sta-
tus of each acquisition, including the current
acquisition phase, the date of the last review,
and a listing of the required documents that
have been reviewed with the dates reviewed or
approved.

“(C) The most current, approved acquisi-
tion program baseline (including project sched-
ules and events).

“(D) A comparison of the original acquisi-
tion program baseline, the current acquisition
program baseline, and the current estimate.
“(E) Whether or not an independent verification and validation has been implemented, with an explanation for the decision and a summary of any findings.

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

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

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

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

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

(b) CLERICAL AMENDMENT.—The table of contents in section 1(b) of the Homeland Security Act of 2002 (6
U.S.C. 101 et seq.) is further amended by adding after the item relating to section 839 the following new item:

"Sec. 840. Acquisition reports."

SEC. 1464. GOVERNMENT ACCOUNTABILITY OFFICE REVIEW OF MULTIYEAR ACQUISITION STRATEGY.

(a) REVIEW REQUIRED.—After submission to Congress of the first multiyear acquisition strategy (pursuant to section 839 of the Homeland Security Act of 2002) after the date of the enactment of this Act, the Comptroller General of the United States shall conduct a review of the plan within 180 days to analyze the viability of the plan’s effectiveness in the following:

(1) Complying with the requirements in section 839 of the Homeland Security Act of 2002, as added by section 1462 of this title.

(2) Establishing clear connections between Department objectives and acquisition priorities.

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

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

(5) Considering potential cost savings through using already-existing technologies when developing acquisition program requirements.
(6) Preventing duplication within Department acquisition workforce training requirements through leveraging already-existing training within the Federal Government, academic community, or private industry.

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

(8) Maximizing small business utilization in acquisitions by, to the maximum extent practicable, ensuring strategic sourcing vehicles seek to increase participation by small businesses, including small and disadvantaged business.

(9) Assessing the feasibility of conducting a pilot program to establish a Homeland Security Acquisition Workforce Development Fund.

(b) REPORT REQUIRED.—The Comptroller General shall submit to the congressional homeland security committees a report on the review required by this section. The report shall be submitted in unclassified form but may include a classified annex.

SEC. 1465. OFFICE OF INSPECTOR GENERAL REPORT.

(a) REVIEW REQUIRED.—No later than 2 years following the submission of the report submitted by the
Comptroller General of the United States as required by section 1464, the Department’s Inspector General shall conduct a review of whether the Department has complied with the multiyear acquisition strategy (pursuant to section 839 of the Homeland Security Act of 2002) and adhered to the strategies set forth in the plan. The review shall also consider whether the Department has complied with the requirements to provide the Acquisition Review Board with a capability development plan for each major acquisition program.

(b) REPORT REQUIRED.—The Inspector General shall submit to the congressional homeland security committees a report of the review required by this section. The report shall be submitted in unclassified form but may include a classified annex.

TITLE XV—QUADRENNIAL HOMELAND SECURITY REVIEW TECHNICAL CORRECTION

SEC. 1501. TECHNICAL CORRECTIONS TO QUADRENNIAL HOMELAND SECURITY REVIEW.

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

(1) in subsection (a)(3)—
(A) in subparagraph (B), by striking "and";
(B) by redesignating subparagraph (C) as subparagraph (D); and
(C) by inserting after subparagraph (B) the following new subparagraph (C):
"(C) representatives from appropriate advisory committees established pursuant to section 871 of this Act, including the Homeland Security Advisory Council and the Homeland Security Science and Technology Advisory Committee, or otherwise established, including the Aviation Security Advisory Committee established pursuant to section 44946 of title 49, United States Code; and"
(2) in subsection (b)—
(A) in paragraph (2), by inserting before the semicolon at the end the following: "based on the risk assessment required pursuant to subsection (c)(2)(B)"
(B) in paragraph (3)—
(i) by inserting "to the extent practicable," after "describe"; and
(ii) by striking "budget plan" and inserting "resources required";
(C) in paragraph (4)—

(i) by inserting “, to the extent practicable,” after “identify”;

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

(iii) by striking the semicolon after “paragraph (2)” and inserting “, including any resources identified from redundant, wasteful, or unnecessary capabilities and capacities that can be redirected to better support other existing capabilities and capacities; and”;

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

(E) by striking paragraph (6);

(3) in subsection (c)—

(A) in paragraph (1)—

(i) by striking “December 31 of the year” and inserting “60 days after the date of the submittal of the President’s budget for the fiscal year after the fiscal year”; and
(ii) by striking “conducted” and inserting “required under subsection (a)(1)”;

(B) in paragraph (2)—

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

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

(iii) in subparagraph (D), by inserting “to the extent practicable,” before “a description”;

(iv) in subparagraph (F)—

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

(II) by striking “the status of”; 

(v) in subparagraph (G)—

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

(II) by striking “the status of”; 

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

(IV) by inserting “and” after the semicolon;
(vi) by striking subparagraph (H);

and

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

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

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

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

“(A) Records regarding the consultation carried out pursuant to subsection (a)(3), including—

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

“(ii) information on how feedback received by the Secretary informed the quadrennial homeland security review.
“(B) Information regarding the risk assessment, as required under subsection (c)(2)(B), including—

“(i) the risk model utilized to generate the risk assessment;

“(ii) information, including data used in the risk model, utilized to generate the risk assessment;

“(iii) sources of information, including other risk assessments, utilized to generate the risk assessment; and

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

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

“(e) REVIEW.—Not later than 90 days after the submission of the report pursuant to subsection (c)(1), the Secretary shall provide to the Committee on Homeland Security of the House of Representatives and the Committee on Homeland Security and Governmental Affairs of the Senate information on the degree to which the findings and recommendations developed in the review were inte-
grated into the acquisition strategy and expenditure plans
for the Department.”.

(b) EFFECTIVE DATE.—The amendments made by
this title shall apply with respect to a quadrennial home-
land security review required to be submitted after Decem-

TITLE XVI—TERRORIST AND
FOREIGN FIGHTER TRAVEL
EXERCISE

SEC. 1601. EXERCISE ON TERRORIST AND FOREIGN FIGHT-
ER TRAVEL.

(a) IN GENERAL.—In addition to, or as part of exer-
cise programs currently carried out by the Department of
Homeland Security, to enhance domestic preparedness for
and collective response to terrorism, promote the dissemi-
nation of homeland security information, and test the se-
curity posture of the United States, the Secretary of
Homeland Security, through appropriate offices and com-
ponents of the Department and in coordination with the
relevant Federal departments and agencies, shall, not later
than one year after the date of the enactment of this Act,
develop and conduct an exercise related to the terrorist
and foreign fighter threat.

(b) EXERCISE REQUIREMENTS.—The exercise re-
quired under subsection (a) shall include—
(1) a scenario involving—

(A) persons traveling from the United States to join or provide material support or resources to a terrorist organization abroad; and

(B) terrorist infiltration into the United States, including United States citizens and foreign nationals; and

(2) coordination with appropriate Federal departments and agencies, foreign governments, and State, local, tribal, territorial, and private sector stakeholders.

(c) REPORT.—Not later than 60 days after the completion of the exercise required under subsection (a), the Secretary of Homeland Security shall, consistent with the protection of classified information, submit an after-action report to the Committee on Homeland Security of the House of Representatives and the Committee on Homeland Security and Governmental Affairs of the Senate presenting the initial findings of such exercise, including any identified or potential vulnerabilities in United States defenses and any legislative changes requested in light of the findings. The report shall be submitted in unclassified form, but may include a classified annex.
(d) PROHIBITION ON ADDITIONAL FUNDING.—No additional funds are authorized to be appropriated to carry out this section.

(e) DEFINITION.—In this section, the term “material support or resources” has the meaning given such term in section 2339A of title 18, United States Code.

SEC. 1602. EMERGING THREATS IN THE NATIONAL EXERCISE PROGRAM.

Subparagraph (A) of section 648(b)(2) of the Post-Katrina Emergency Management Reform Act of 2006 (6 U.S.C. 748(b)(2)) is amended—

(1) in clause (v), by striking “and” at the end; and

(2) by adding after clause (vi) the following new clause:

“(vii) designed, to the extent practicable, to include exercises addressing emerging terrorist threats, such as scenarios involving United States citizens departing the United States to enlist with or provide material support or resources to terrorist organizations abroad or terrorist infiltration into the United States, including United States citizens and foreign nationals; and”.
TITLE XVII—AIRPORT PERIMETER AND ACCESS CONTROL SECURITY

SEC. 1701. RISK ASSESSMENTS OF AIRPORT SECURITY.

(a) In General.—The Administrator of the Transportation Security Administration (TSA) shall—

(1) not later than 60 days after the date of the enactment of this Act, update the Transportation Sector Security Risk Assessment (TSSRA) for the aviation sector; and

(2) not later than 90 days after such date—

(A) update with the latest and most currently available intelligence information the Comprehensive Risk Assessment of Perimeter and Access Control Security (in this title referred to as the “Risk Assessment of Airport Security”) and determine a regular timeframe and schedule for further updates to such Risk Assessment of Airport Security; and

(B) conduct a system-wide assessment of airport access control points and airport perimeter security.

(b) Contents.—The security risk assessments required under subsection (a)(2) shall—
(1) include updates reflected in the TSSRA and Joint Vulnerability Assessment (JVA) findings;
(2) reflect changes to the risk environment relating to airport access control points and airport perimeters;
(3) use security event data for specific analysis of system-wide trends related to airport access control points and airport perimeter security to better inform risk management decisions; and
(4) take into consideration the unique geography of and current best practices used by airports to mitigate potential vulnerabilities.

(e) Report.—The Administrator of the Transportation Security Administration shall report to the Committee on Homeland Security of the House of Representatives and the Committee on Homeland Security and Governmental Affairs and the Committee on Commerce, Science, and Transportation of the Senate, relevant Federal departments and agencies, and airport operators on the results of the security risk assessments required under subsection (a).

SEC. 1702. AIRPORT SECURITY STRATEGY DEVELOPMENT.

(a) In General.—Not later than 90 days after the date of the enactment of this Act, the Administrator of the Transportation Security Administration shall update
the 2012 National Strategy for Airport Perimeter and Access Control Security (in this section referred to as the “National Strategy”).

(b) CONTENTS.—The update to the National Strategy required under subsection (a) shall include—

(1) information from the Risk Assessment of Airport Security; and

(2) information on—

(A) airport security-related activities;

(B) the status of TSA efforts to address the goals and objectives referred to in subsection (a);

(C) finalized outcome-based performance measures and performance levels for each relevant activity and goal and objective under subparagraphs (A) and (B); and

(D) input from airport operators.

(c) UPDATES.—Not later than 90 days after the update is completed under subsection (a), the Administrator of the Transportation Security Administration shall implement a process for determining when additional updates to the strategy referred to in such subsection are needed.
TITLE XVIII—COMMUNITY COUNTERTERRORISM PREPAREDNESS

SEC. 1801. MAJOR METROPOLITAN AREA COUNTERTERRORISM TRAINING AND EXERCISE GRANT PROGRAM.

(a) In general.—Subtitle A of title XX of the Homeland Security Act of 2002 (6 U.S.C. 603 et seq.) is amended by adding at the end the following new section:

“SEC. 2009. MAJOR METROPOLITAN AREA COUNTERTERRORISM TRAINING AND EXERCISE GRANT PROGRAM.

“(a) Establishment.—

“(1) In general.—The Secretary, acting through the Administrator and the heads of other relevant components of the Department, shall carry out a program for emergency response providers to prevent, prepare for, and respond to the most likely terrorist attack scenarios, including active shooters, as determined by the Secretary, against major metropolitan areas.

“(2) Information.—In establishing the program under paragraph (1), the Secretary shall provide to eligible applicants—
“(A) information, in an unclassified format, on the most likely terrorist attack scenarios, including active shooters, which such grants are intended to address; and

“(B) information on training and exercises best practices.

“(b) ELIGIBLE APPLICANTS.—

“(1) IN GENERAL.—Emergency response providers in jurisdictions that are currently receiving, or that previously received, funding under section 2003 may apply for a grant under the program established in subsection (a).

“(2) ADDITIONAL JURISDICTIONS.—Eligible applicants receiving funding under the program established in subsection (a) may include in activities funded by such program neighboring jurisdictions that would be likely to provide mutual aid in response to the most likely terrorist attack scenarios, including active shooters.

“(c) APPLICATION.—

“(1) IN GENERAL.—Eligible applicants described in subsection (b) may apply for a grant under this section, and shall submit such information in support of an application as the Administrator may require.
“(2) Minimum Contents of Application.—

The Administrator shall require that each applicant include in its application at a minimum, the following:

“(A) The purpose for which the applicant seeks grant funds, including a description of how the applicant plans to use such funds.

“(B) A description of how the activity for which the funding is sought will prepare the applicant to prevent, prepare for, and respond to complex, coordinated attacks.

“(C) A description of how the applicant will work with community partners located within the applicant’s jurisdiction, such as schools, places of worship, and businesses, as appropriate, when conducting activities permitted under subsection (d).

“(D) Such other information as determined necessary by the Administrator.

“(d) Permitted Uses.—The recipient of a grant under this section may use such grant to conduct training and exercises consistent with preventing, preparing for, and responding to the most likely terrorist attack scenarios, including active shooters.
“(e) Period of Performance.—The Administrator shall make funds provided under this section available for use by a recipient of a grant for a period of not fewer than 24 months.

“(f) Authorization of Appropriations.—There are authorized to be appropriated for grants under this section $39,000,000 for each of fiscal years 2017 through 2022.”.

(b) Clerical Amendment.—The table of contents in section 1(b) of the Homeland Security Act of 2002 is amended by inserting after the item relating to section 2008 the following new item:

“Sec. 2009. Major metropolitan area counterterrorism training and exercise grant program.”.

TITLE XIX—CYBER PREPAREDNESS

SEC. 1901. INFORMATION SHARING.

Title II of the Homeland Security Act of 2002 is amended—

(1) in section 210A (6 U.S.C. 124h)—

(A) in subsection (b)—

(i) in paragraph (10), by inserting before the semicolon at the end the following: “, including, in coordination with the national cybersecurity and communications integration center under section 227, ac-
cessing timely technical assistance, risk management support, and incident response capabilities with respect to cyber threat indicators, defensive measures, cybersecurity risks, and incidents (as such terms are defined in such section), which may include attribution, mitigation, and remediation, and the provision of information and recommendations on security and resilience, including implications of cybersecurity risks to equipment and technology related to the electoral process”;

(ii) in paragraph (11), by striking “and” after the semicolon;

(iii) by redesignating paragraph (12) as paragraph (14); and

(iv) by inserting after paragraph (11) the following new paragraphs:

“(12) review information relating to cybersecurity risks that is gathered by State, local, and regional fusion centers, and incorporate such information, as appropriate, into the Department’s own information relating to cybersecurity risks;
“(13) ensure the dissemination to State, local, and regional fusion centers of information relating to cybersecurity risks; and”;

(B) in subsection (c)(2)—

(i) by redesignating subparagraphs (C) through (G) as subparagraphs (D) through (H), respectively; and

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

“(C) The national cybersecurity and communications integration center under section 227.”;

(C) in subsection (d)—

(i) in paragraph (3), by striking “and” after the semicolon;

(ii) by redesignating paragraph (4) as paragraph (5); and

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

“(4) assist, in coordination with the national cybersecurity and communications integration center under section 227, fusion centers in using information relating to cybersecurity risks to develop a comprehensive and accurate threat picture; and”; and

(D) in subsection (j)—
(i) by redesignating paragraphs (1) through (5) as paragraphs (2) through (6), respectively; and

(ii) by inserting before paragraph (2), as so redesignated, the following new paragraph:

“(1) the term ‘cybersecurity risk’ has the meaning given that term in section 227;”; and

(2) in section 227 (6 U.S.C. 148)—

(A) in subsection (e)—

(i) in paragraph (5)(B), by inserting ‘‘, including State and major urban area fusion centers, as appropriate’’ before the semicolon at the end;

(ii) in paragraph (7), in the matter preceding subparagraph (A), by striking ‘‘information and recommendations’’ each place it appears and inserting ‘‘information, recommendations, and best practices’’; and

(iii) in paragraph (9), by inserting ‘‘and best practices’’ after ‘‘defensive measures’’; and

(B) in subsection (d)(1)(B)(ii), by inserting ‘‘and State and major urban area fusion
centers, as appropriate” before the semicolon at the end.

SEC. 1902. HOMELAND SECURITY GRANTS.

Subsection (a) of section 2008 of the Homeland Security Act of 2002 (6 U.S.C. 609) is amended—

(1) by redesignating paragraphs (4) through (14) as paragraphs (5) through (15), respectively; and

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

“(4) enhancing cybersecurity, including preparing for and responding to cybersecurity risks and incidents and developing State-wide cyber threat information analysis and dissemination activities;”.

SEC. 1903. SENSE OF CONGRESS.

It is the sense of Congress that to facilitate the timely dissemination to appropriate State, local, and private sector stakeholders of homeland security information related to cyber threats, the Secretary of Homeland Security should, to the greatest extent practicable, work to share actionable information related to cyber threats in an unclassified form.
TITLE XX—TRANSIT SECURITY
GRANT PROGRAM FLEXIBILITY

SEC. 2001. ALLOWABLE USES OF FUNDS FOR PUBLIC TRANSPORTATION SECURITY ASSISTANCE GRANTS.

Subparagraph (A) of section 1406(b)(2) of the Implementing Recommendations of the 9/11 Commission Act of 2007 (6 U.S.C. 1135(b)(2); Public Law 110–53) is amended by inserting “and associated backfill” after “security training”.

SEC. 2002. PERIODS OF PERFORMANCE FOR PUBLIC TRANSPORTATION SECURITY ASSISTANCE GRANTS.


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

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

“(m) PERIODS OF PERFORMANCE.—

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

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

SEC. 2003. GAO REVIEW.


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

(1) An assessment of the type of projects funded under the transit security grant program.

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

(3) An assessment of the impact, if any, of this title (including the amendments made by this title) on types of projects funded under the transit security grant program.
(4) An assessment of the management and administration of transit security grant program funds by grantees.

(5) Recommendations to improve the manner in which transit security grant program funds address vulnerabilities in transportation infrastructure.

(6) Recommendations to improve the management and administration of the transit security grant program.

(c) REPORT.—Not later than 1 year after the date of the enactment of this Act and again not later than five years after such date of enactment, the Comptroller General shall submit to the Committee on Homeland Security of the House of Representatives and the Committee on Homeland Security and Governmental Affairs of the Senate a report on the review required under this section.

TITLE XXI—SUPPORT FOR RAPID INNOVATION

SEC. 2101. CYBERSECURITY RESEARCH AND DEVELOPMENT PROJECTS.

(a) CYBERSECURITY RESEARCH AND DEVELOPMENT.—

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

“SEC. 319. CYBERSECURITY RESEARCH AND DEVELOPMENT.

“(a) IN GENERAL.—The Under Secretary for Science and Technology shall support the research, development, testing, evaluation, and transition of cybersecurity technologies, including fundamental research to improve the sharing of information, analytics, and methodologies related to cybersecurity risks and incidents, consistent with current law.

“(b) ACTIVITIES.—The research and development supported under subsection (a) shall serve the components of the Department and shall—

“(1) advance the development and accelerate the deployment of more secure information systems;

“(2) improve and create technologies for detecting attacks or intrusions, including real-time continuous diagnostics and real-time analytic technologies;

“(3) improve and create mitigation and recovery methodologies, including techniques and policies for real-time containment of attacks, and development of resilient networks and information systems;
“(4) support, in coordination with non-Federal entities, the review of source code that underpins critical infrastructure information systems;

“(5) develop and support infrastructure and tools to support cybersecurity research and development efforts, including modeling, testbeds, and data sets for assessment of new cybersecurity technologies;

“(6) assist the development and support of technologies to reduce vulnerabilities in industrial control systems; and

“(7) develop and support cyber forensics and attack attribution capabilities.

“(c) COORDINATION.—In carrying out this section, the Under Secretary for Science and Technology shall coordinate activities with—

“(1) the Under Secretary appointed pursuant to section 103(a)(1)(H);

“(2) the heads of other relevant Federal departments and agencies, as appropriate; and

“(3) industry and academia.

“(d) TRANSITION TO PRACTICE.—The Under Secretary for Science and Technology shall support projects carried out under this title through the full life cycle of such projects, including research, development, testing,
evaluation, pilots, and transitions. The Under Secretary shall identify mature technologies that address existing or imminent cybersecurity gaps in public or private information systems and networks of information systems, identify and support necessary improvements identified during pilot programs and testing and evaluation activities, and introduce new cybersecurity technologies throughout the homeland security enterprise through partnerships and commercialization. The Under Secretary shall target federally funded cybersecurity research that demonstrates a high probability of successful transition to the commercial market within 2 years and that is expected to have a notable impact on the public or private information systems and networks of information systems.

“(e) DEFINITIONS.—In this section:

“(1) CYBERSECURITY RISK.—The term ‘cybersecurity risk’ has the meaning given such term in section 227.

“(2) HOMELAND SECURITY ENTERPRISE.—The term ‘homeland security enterprise’ means relevant governmental and nongovernmental entities involved in homeland security, including Federal, State, local, and tribal government officials, private sector representatives, academics, and other policy experts.
“(3) INCIDENT.—The term ‘incident’ has the
meaning given such term in section 227.

“(4) INFORMATION SYSTEM.—The term ‘infor-
mation system’ has the meaning given such term in
section 3502(8) of title 44, United States Code.”.

(2) CLERICAL AMENDMENT.—The table of con-
tents in section 1(b) of the Homeland Security Act
of 2002 is amended by inserting after the item relat-
ing to section 318 the following new item:

“Sec. 319. Cybersecurity research and development.”.

(b) RESEARCH AND DEVELOPMENT PROJECTS.—
Section 831 of the Homeland Security Act of 2002 (6
U.S.C. 391) is amended—

(1) in subsection (a)—

(A) in the matter preceding paragraph (1),
by striking “2016” and inserting “2020”;

(B) in paragraph (1), by striking the last
sentence; and

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

“(3) PRIOR APPROVAL.—In any case in which
the head of a component or office of the Department
seeks to utilize the authority under this section, such
head shall first receive prior approval from the Sec-
retary by providing to the Secretary a proposal that
includes the rationale for the utilization of such au-
authority, the funds to be spent on the use of such au-
thority, and the expected outcome for each project
that is the subject of the use of such authority. In
such a case, the authority for evaluating the prop-
posal may not be delegated by the Secretary to any-
one other than the Under Secretary for Manage-
ment.”;

(2) in subsection (c)—

(A) in paragraph (1), in the matter pre-
ceeding subparagraph (A), by striking “2016”
and inserting “2020”; and

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

“(2) REPORT.—The Secretary shall annually
submit to the Committee on Homeland Security and
the Committee on Science, Space, and Technology of
the House of Representatives and the Committee on
Homeland Security and Governmental Affairs of the
Senate a report detailing the projects for which the
authority granted by subsection (a) was utilized, the
rationale for such utilizations, the funds spent uti-
lizing such authority, the extent of cost-sharing for
such projects among Federal and non-Federal
sources, the extent to which utilization of such au-
thority has addressed a homeland security capability

gap or threat to the homeland identified by the Department, the total amount of payments, if any, that were received by the Federal Government as a result of the utilization of such authority during the period covered by each such report, the outcome of each project for which such authority was utilized, and the results of any audits of such projects.”; and

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

“(e) TRAINING.—The Secretary shall develop a training program for acquisitions staff on the utilization of the authority provided under subsection (a).”.

(c) PROHIBITION ON ADDITIONAL FUNDING.—No additional funds are authorized to be appropriated to carry out this title and the amendments made by this title.

TITLE XXII—LEVERAGING EMERGING TECHNOLOGIES

SEC. 2201. INNOVATION ENGAGEMENT.

(a) INNOVATION ENGAGEMENT.—

(1) IN GENERAL.—The Secretary of Homeland Security—

(A) shall engage with innovative and emerging technology developers and firms, including technology-based small businesses and
startup ventures, to address homeland security
needs; and

(B) may identify geographic areas in the
United States with high concentrations of such
innovative and emerging technology developers
and firms, and may establish personnel and of-

(2) ENGAGEMENT.—Engagement under para-
graph (1) may include innovative and emerging tech-
nology developers or firms with proven technologies,
supported with outside investment, with potential
applications for the Department of Homeland Secu-

(3) CO-LOCATION.—If the Secretary of Home-
land Security determines that it is appropriate to es-

(A) the Department of Homeland Security,

(B) Federal facilities, where appropriate.

(4) OVERSIGHT.—Not later than 30 days after
establishing personnel and office space in a specific
geographic area in the United States pursuant to paragraph (1)(B), the Secretary of Homeland Security shall inform Congress about the rationale for such establishment, the anticipated costs associated with such establishment, and the specific goals for such establishment.

(b) STRATEGIC PLAN.—Not later than 6 months after the date of the enactment of this section, the Secretary of Homeland Security shall develop, implement, and submit to the Committee on Homeland Security of the House of Representatives and the Committee on Homeland Security and Governmental Affairs of the Senate a Department of Homeland Security-wide strategy to proactively engage with innovative and emerging technology developers and firms, including technology-based small businesses and startup ventures, in accordance with subsection (a). Such strategy shall—

(1) focus on sustainable methods and guidance to build relationships, including with such innovative and emerging technology developers and firms in geographic areas in the United States with high concentrations of such innovative and emerging technology developers and firms, and in geographic areas outside such areas, to establish, develop, and en-
hance departmental capabilities to address homeland
security needs;

(2) include efforts to—

(A) ensure proven innovative and emerging
technologies can be included in existing and fu-
ture acquisition contracts;

(B) coordinate with organizations that pro-
vide venture capital to businesses, particularly
small businesses and startup ventures, as ap-
propriate, to assist the commercialization of in-
novative and emerging technologies that are ex-
pected to be ready for commercialization in the
near term and within 36 months; and

(C) address barriers to the utilization of
innovative and emerging technologies and the
engagement of small businesses and startup
ventures in the acquisition process;

(3) include a description of how the Depart-
ment plans to leverage proven innovative and emerg-
ing technologies to address homeland security needs;

and

(4) include the criteria the Secretary plans to
use to determine an innovative or technology is prov-
en.
(c) Prohibition on Additional Funding.—No additional funds are authorized to be appropriated to carry out this title.

**TITLE XXIII—FIRST RESPONDER ACCESS TO INNOVATIVE TECHNOLOGIES**

**SEC. 2301.** Approval of certain equipment.

(a) In General.—Subsection (f) of section 2008 of the Homeland Security Act of 2002 (6 U.S.C. 609) is amended—

(1) by striking “If an applicant” and inserting the following:

“(1) Application requirement.—If an applicant”; and

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

“(2) Review process.—The Administrator shall implement a uniform process for reviewing applications that, in accordance with paragraph (1), contain explanations to use grants provided under section 2003 or 2004 to purchase equipment or systems that do not meet or exceed any applicable national voluntary consensus standards developed under section 647 of the Post-Katrina Emergency Management Reform Act of 2006 (6 U.S.C. 747).
“(3) FACTORS.—In carrying out the review process under paragraph (2), the Administrator shall consider the following:

“(A) Current or past use of proposed equipment or systems by Federal agencies or the Armed Forces.

“(B) The absence of a national voluntary consensus standard for such equipment or systems.

“(C) The existence of an international consensus standard for such equipment or systems, and whether such equipment or systems meets such standard.

“(D) The nature of the capability gap identified by the applicant and how such equipment or systems will address such gap.

“(E) The degree to which such equipment or systems will serve the needs of the applicant better than equipment or systems that meet or exceed existing consensus standards.

“(F) Any other factor determined appropriate by the Administrator.”.

(b) INSPECTOR GENERAL REPORT.—Not later than 3 years after the date of the enactment of this Act, the Inspector General of the Department of Homeland Secu-
rity shall submit to the Committee on Homeland Security of the House of Representatives and the Committee on Homeland Security and Governmental Affairs of the Senate a report assessing the implementation of the review process established under paragraph (2) of subsection (f) of section 2008 of the Homeland Security Act of 2002 (as added by subsection (a) of this section), including information on the following:

(1) The number of requests to purchase equipment or systems that do not meet or exceed any applicable consensus standard evaluated under such review process.

(2) The capability gaps identified by applicants and the number of such requests granted or denied.

(3) The processing time for the review of such requests.
TITLE XXIV—DEPARTMENT OF HOMELAND SECURITY STRATEGY FOR INTERNATIONAL PROGRAMS

SEC. 2401. COMPREHENSIVE STRATEGY FOR INTERNATIONAL PROGRAMS FOR VETTING AND SCREENING PERSONS SEEKING TO ENTER THE UNITED STATES.

(a) IN GENERAL.—Not later than 180 days after the date of the enactment of this Act, the Secretary of Homeland Security shall submit to the Committee on Homeland Security of the House of Representatives and the Committee on Homeland Security and Governmental Affairs of the Senate a comprehensive 3-year strategy for international programs of the Department of Homeland Security in which personnel and resources of the Department are deployed abroad for vetting and screening of persons seeking to enter the United States.

(b) CONTENTS.—The strategy required under subsection (a) shall include, at a minimum, the following:

(1) Specific Department of Homeland Security risk-based goals for international programs of the Department in which personnel and resources of the Department are deployed abroad for vetting and screening of persons seeking to enter the United States.
screening of persons seeking to enter the United States.

(2) A risk-based method for determining whether to establish new international programs in new locations, given resource constraints, or expand existing international programs of the Department, in which personnel and resources of the Department are deployed abroad for vetting and screening of persons seeking to enter the United States.

(3) Alignment with the highest Department-wide and Government-wide strategic priorities of resource allocations on international programs of the Department in which personnel and resources of the Department are deployed abroad for vetting and screening of persons seeking to enter the United States.

(4) A common reporting framework for the submission of reliable, comparable cost data by components of the Department on overseas expenditures attributable to international programs of the Department in which personnel and resources of the Department are deployed abroad for vetting and screening of persons seeking to enter the United States.
(c) CONSIDERATIONS.—In developing the strategy required under subsection (a), the Secretary of Homeland Security shall consider, at a minimum, the following:

(1) Information on existing operations of international programs of the Department of Homeland Security in which personnel and resources of the Department are deployed abroad for vetting and screening of persons seeking to enter the United States that includes corresponding information for each location in which each such program operates.

(2) The number of Department personnel deployed to each location at which an international program referred to in subparagraph (A) is in operation during the current and preceding fiscal year.

(3) Analysis of the impact of each international program referred to in paragraph (1) on domestic activities of components of the Department of Homeland Security.

(4) Analysis of barriers to the expansion of an international program referred to in paragraph (1).

(d) FORM.—The strategy required under subsection (a) shall be submitted in unclassified form but may contain a classified annex if the Secretary of Homeland Security determines that such is appropriate.
TITLE XXV—DHS STOP ASSET
AND VEHICLE EXCESS

SEC. 2601. DHS VEHICLE FLEETS.


(1) in subsection (a)(5), by inserting “vehicle fleets (under subsection (c)),” after “equipment,”;

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

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

“(c) VEHICLE FLEETS.—

“(1) IN GENERAL.—In carrying out responsibilities regarding vehicle fleets pursuant to subsection (a)(5), the Under Secretary for Management shall be responsible for overseeing and managing vehicle fleets throughout the Department. The Under Secretary shall also be responsible for the following:

“(A) Ensuring that components are in compliance with Federal law, Federal regulations, executive branch guidance, and Department policy (including issuing guidance relating to such) relating to fleet management and use of vehicles from home to work.
“(B) Developing and distributing a standardized vehicle allocation methodology and fleet management plan for components to use to determine optimal fleet size in accordance with paragraph (4).

“(C) Ensuring that components formally document fleet management decisions.

“(D) Approving component fleet management plans, vehicle leases, and vehicle acquisitions.

“(2) COMPONENT RESPONSIBILITIES.—

“(A) IN GENERAL.—Component heads—

“(i) shall—

“(I) comply with Federal law, Federal regulations, executive branch guidance, and Department policy (including guidance relating to such) relating to fleet management and use of vehicles from home to work;

“(II) ensure that data related to fleet management is accurate and reliable;

“(III) use such data to develop a vehicle allocation tool derived by using the standardized vehicle allocation
methodology provided by the Under Secretary for Management to determine the optimal fleet size for the next fiscal year and a fleet management plan; and

“(IV) use vehicle allocation methodologies and fleet management plans to develop annual requests for funding to support vehicle fleets pursuant to paragraph (6); and

“(ii) may not, except as provided in subparagraph (B), lease or acquire new vehicles or replace existing vehicles without prior approval from the Under Secretary for Management pursuant to paragraph (5)(B).

“(B) Exception regarding certain leasing and acquisitions.—If exigent circumstances warrant such, a component head may lease or acquire a new vehicle or replace an existing vehicle without prior approval from the Under Secretary for Management. If under exigent circumstances a component head so leases, acquires, or replaces a vehicle, such component
head shall provide to the Under Secretary an explanation of such circumstances.

“(3) ONGOING OVERSIGHT.—

“(A) QUARTERLY MONITORING.—In accordance with paragraph (4), the Under Secretary for Management shall collect, on a quarterly basis, information regarding component vehicle fleets, including information on fleet size, composition, cost, and vehicle utilization.

“(B) AUTOMATED INFORMATION.—The Under Secretary for Management shall seek to achieve a capability to collect, on a quarterly basis, automated information regarding component vehicle fleets, including the number of trips, miles driven, hours and days used, and the associated costs of such mileage for leased vehicles.

“(C) MONITORING.—The Under Secretary for Management shall track and monitor component information provided pursuant to subparagraph (A) and, as appropriate, subparagraph (B), to ensure that component vehicle fleets are the optimal fleet size and cost effective. The Under Secretary shall use such infor-
mation to inform the annual component fleet analyses referred to in paragraph (4).

“(4) ANNUAL REVIEW OF COMPONENT FLEET ANALYSES.—

“(A) IN GENERAL.—To determine the optimal fleet size and associated resources needed for each fiscal year beginning with fiscal year 2018, component heads shall annually submit to the Under Secretary for Management a vehicle allocation tool and fleet management plan using information described in paragraph (3)(A). Such tools and plans may be submitted in classified form if a component head determines that such is necessary to protect operations or mission requirements.

“(B) VEHICLE ALLOCATION TOOL.—Component heads develop a vehicle allocation tool in accordance with subclause (III) of paragraph (2)(A)(i) that includes an analysis of the following:

“(i) Vehicle utilization data, including the number of trips, miles driven, hours and days used, and the associated costs of such mileage for leased vehicles, in accordance with such paragraph.
'“(ii) The role of vehicle fleets in supporting mission requirements for each component.

“(iii) Any other information determined relevant by such component heads.

“(C) FLEET MANAGEMENT PLANS.—Component heads shall use information described in subparagraph (B) to develop a fleet management plan for each such component. Such fleet management plans shall include the following:

“(i) A plan for how each such component may achieve optimal fleet size determined by the vehicle allocation tool required under such subparagraph, including the elimination of excess vehicles in accordance with paragraph (5), if applicable.

“(ii) A cost benefit analysis supporting such plan.

“(iii) A schedule each such component will follow to obtain optimal fleet size.

“(iv) Any other information determined relevant by component heads.

“(D) REVIEW.—The Under Secretary for Management shall review and make a determination on the results of each component’s ve-
vehicle allocation tool and fleet management plan under this paragraph to ensure each such com-
ponent’s vehicle fleets are the optimal fleet size and that components are in compliance with ap-
plicable Federal law, Federal regulations, executive branch guidance, and Department policy pursuant to paragraph (2) relating to fleet management and use of vehicles from home to work. The Under Secretary shall use such tools and plans when reviewing annual component re-
quests for vehicle fleet funding in accordance with paragraph (6).

“(5) GUIDANCE TO DEVELOP FLEET MANAGEMENT PLANS.—The Under Secretary for Manage-
ment shall provide guidance, pursuant to paragraph (1)(B) on how component heads may achieve opti-
mal fleet size in accordance with paragraph (4), in-
cluding processes for the following:

“(A) Leasing or acquiring additional vehi-
cles or replacing existing vehicles, if determined necessary.

“(B) Disposing of excess vehicles that the Under Secretary determines should not be re-
allocated under subparagraph (C).
“(C) Reallocating excess vehicles to other components that may need temporary or long-term use of additional vehicles.

“(6) **Annual review of vehicle fleet funding requests.**—As part of the annual budget process, the Under Secretary for Management shall review and make determinations regarding annual component requests for funding for vehicle fleets. If component heads have not taken steps in furtherance of achieving optimal fleet size in the prior fiscal year pursuant to paragraphs (4) and (5), the Under Secretary shall provide rescission recommendations to the Committee on Appropriations and the Committee on Homeland Security of the House of Representatives and the Committee on Appropriations and the Committee on Homeland Security and Governmental Affairs of the Senate regarding such component vehicle fleets.

“(7) **Accountability for vehicle fleet management.**—

“(A) **Prohibition on certain new vehicle leases and acquisitions.**—The Under Secretary for Management and component heads may not approve in any fiscal year beginning with fiscal year 2019 a vehicle lease, ac-
quisition, or replacement request if such compo-
nent heads did not comply in the prior fiscal
year with paragraph (4).

“(B) Prohibition on certain perform-
ance compensation.—No Department official
with vehicle fleet management responsibilities
may receive annual performance compensation
in pay in any fiscal year beginning with fiscal
year 2019 if such official did not comply in the
prior fiscal year with paragraph (4).

“(C) Prohibition on certain car serv-
ices.—Notwithstanding any other provision of
law, no senior executive service official of the
Department whose office has a vehicle fleet may
receive access to a car service in any fiscal year
beginning with fiscal year 2019 if such official
did not comply in the prior fiscal year with
paragraph (4).

“(8) Motor pool.—

“(A) In general.—The Under Secretary
for Management may determine the feasibility
of operating a vehicle motor pool to permit
components to share vehicles as necessary to
support mission requirements to reduce the
number of excess vehicles in the Department.
“(B) REQUIREMENTS.—The determination of feasibility of operating a vehicle motor pool under subparagraph (A) shall—

“(i) include—

“(I) regions in the United States in which multiple components with vehicle fleets are located in proximity to one another, or a significant number of employees with authorization to use vehicles are located; and

“(II) law enforcement vehicles;

“(ii) cover the National Capital Region; and

“(iii) take into account different mission requirements.

“(C) REPORT.—The Secretary shall include in the Department’s next annual performance report required under current law the results of the determination under this paragraph.

“(9) DEFINITIONS.—In this subsection:

“(A) COMPONENT HEAD.—The term ‘component head’ means the head of any component of the Department with a vehicle fleet.
“(B) EXCESS VEHICLE.—The term ‘excess vehicle’ means any vehicle that is not essential to support mission requirements of a component.

“(C) OPTIMAL FLEET SIZE.—The term ‘optimal fleet size’ means, with respect to a particular component, the appropriate number of vehicles to support mission requirements of such component.

“(D) VEHICLE FLEET.—The term ‘vehicle fleet’ means all owned, commercially leased, or Government-leased vehicles of the Department or of a component of the Department, as the case may be, including vehicles used for law enforcement and other purposes.”.

SEC. 2602. GAO REPORT AND INSPECTOR GENERAL REVIEW.

(a) GAO REPORT.—Not later than 1 year after the date of the enactment of this Act, the Comptroller General of the United States shall submit to the Committee on Homeland Security of the House of Representatives and the Committee on Homeland Security and Governmental Affairs a report on the following:

(1) The status of efforts at achieving a capability to collect automated information as required
under subsection (c)(3) of section 701 of the Homeland Security Act of 2002 (6 U.S.C. 341), as added by section 2601 of this title, and any challenges that remain with respect to achieving the capability to collect, assess, and report vehicle fleet (as such term in defined in subsection (c)(9) of such section 701) data for the purpose of determining vehicle utilization.

(2) The extent to which the Under Secretary for Management has identified and addressed any relevant security concerns, including cybersecurity risks, related to such automation.

(3) The extent to which the Under Secretary collects, assesses, and reports on vehicle fleet event data recorder data.

(b) INSPECTOR GENERAL REVIEW.—The Inspector General of the Department of Homeland Security shall—

(1) review implementation of subsection (c)(4) of section 701 of the Homeland Security Act of 2002 (6 U.S.C. 341), as added by section 2601 of this title, for fiscal years 2018 and 2020, and shall provide, upon request, to the Committee on Homeland Security of the House of Representatives and the Committee on Homeland Security and Govern-
mental Affairs of the Senate information regarding any such review; and

(2) submit to the committees specified in paragraph (1) a report, not later than 6 months after completion of the second review required under such paragraph, regarding the effectiveness of such subsection with respect to cost avoidance, savings realized, and component operations.

TITLE XXVI—COUNTERTERRORISM SCREENING AND ASSISTANCE

SEC. 2601. FOREIGN PARTNER ENGAGEMENT PLAN.

(a) FINDINGS.—Consistent with the final report of the Committee on Homeland Security of the House of Representatives bipartisan “Task Force on Combating Terrorist and Foreign Fighter Travel”, Congress makes the following findings:

(1) It is important for the national security of the United States to assist foreign partners in closing security gaps which may allow terrorists and foreign fighters to travel internationally, avoiding detection.

(2) Building foreign partner capacity to combat terrorist travel helps extend the United States secu-
rity beyond its border to mitigate threats before they reach the United States.

(3) United States Government departments and agencies have spent billions of dollars to help foreign partners improve their security against terrorist travel since the attacks of September 11, 2001, including through the provision of technical assistance, equipment, training, and other tools.

(4) The lack of a United States Government-wide, risk-based approach increases the odds that systematic security gaps abroad may persist and that United States response efforts will not be maximized in order to close these gaps.

(5) Failure to effectively coordinate capacity-building activities also results in greater risk of overlap, waste, and unnecessary duplication between the United States and international programs.

(b) Sense of Congress.—It is the sense of Congress that the United States Government must ensure capacity-building assistance is coordinated both among United States Government departments and agencies as well as with foreign implementing partners, and assistance should be prioritized for the highest-risk countries for travel by terrorists and foreign fighters.

(c) Plan.—
(1) IN GENERAL.—Not later than 180 days after the date of the enactment of this Act and every 2 years thereafter at the time of the President’s budget submission to Congress under section 1105 of title 31, United States Code, until 2022, the Secretary of State shall, in accordance with the protection of intelligence sources and methods, develop and submit to the appropriate congressional committees unclassified and classified versions of a foreign partner engagement plan which catalogues existing capacity-building initiatives abroad to combat travel by terrorists and foreign fighters and identifies areas for adjustment to align ongoing efforts with risk-based priorities.

(2) COORDINATION.—The plan required under paragraph (1) shall be developed in coordination with all relevant United States Government departments and agencies and in consultation with the Secretary of Homeland Security, the Secretary of the Treasury, the Secretary of Defense, the Attorney General, the Director of National Intelligence, and the Director of the Federal Bureau of Investigation.

(3) CONTENTS.—The plan required under paragraph (1) shall—
(A) include an assessment of all countries and whether each country is high-risk, medium-risk, or low-risk for travel by terrorists and foreign fighters based on the minimum standards described in section 2603(b), as well as—

(i) an identification of the number of flights that originate from last points of departure in each country to the United States;

(ii) visa waiver program status or visa application and denial rates for each country;

(iii) recent threats, terrorist and foreign fighter travel trends, and the overall terror threat environment in each country; and

(iv) other criteria as determined by the Secretary of State and the Secretary of Homeland Security;

(B) detail existing United States Government programs, projects, and activities which are intended to or have the substantial effect of building the capacity of such countries to combat travel by terrorists and foreign fighters, in-
including estimated spending levels by country where practicable; and

(C) outline a plan for prioritizing United States Government resources toward high-risk and medium-risk countries, including—

(i) identifying efforts which should be reformed, consolidated, or eliminated; and

(ii) detailing new programs, projects, or activities that are requested, being planned, or are undergoing implementation and associated costs.

SEC. 2602. SHARING SYSTEMS AND EQUIPMENT TO OBSTRUCT TRAVEL BY TERRORISTS AND FOREIGN FIGHTERS.

(a) Border Security and Counterterrorism Screening Tools.—

(1) In general.—Subject to subsection (d), the Secretary of Homeland Security and the Secretary of State shall accelerate the provision of appropriate versions of the following systems to foreign governments:

(A) U.S. Customs and Border Protection’s Automated Targeting System—Global.
(B) The Department of State’s Personal Identification Secure Comparison and Evaluation System.

(2) PRIORITIZATION.—The Secretary of Homeland Security and the Secretary of State shall coordinate to prioritize the provision of the systems specified in paragraph (1) to countries determined to be high-risk and medium-risk in the foreign partner engagement plan required under section 2601.

(b) EQUIPMENT TRANSFER.—

(1) IN GENERAL.—Subject to paragraphs (2) and (3), the Secretary of Homeland Security, in consultation with the Secretary of State, is authorized to provide, with or without reimbursement, excess nonlethal equipment and supplies owned by the Department of Homeland Security to a foreign government.

(2) DETERMINATION.—The Secretary of Homeland Security is authorized to provide equipment and supplies pursuant to paragraph (1) if the Secretary determines that the provision of such equipment and supplies would—

(A) further the homeland security interests of the United States; and
(B) enhance the recipient government’s capacity to—

(i) mitigate the risk or threat of terrorism, infectious disease, or natural disaster;

(ii) protect and expedite lawful trade and travel; or

(iii) enforce intellectual property rights.

(3) LIMITATION ON TRANSFER.—The Secretary of Homeland Security may not—

(A) provide any equipment or supplies that are designated as items on the United States Munitions List pursuant to section 38 of the Arms Export Control Act (22 U.S.C. 2778); or

(B) provide any vessel or aircraft pursuant to this subsection.

(4) RELATED TRAINING.—In conjunction with a provision of equipment or supplies pursuant to paragraph (1), the Secretary of Homeland Security may provide such equipment-related or supplies-related training and assistance as the Secretary determines to be necessary.

(5) MAINTENANCE OF TRANSFERRED EQUIPMENT.—The Secretary of Homeland Security may
provide for the maintenance of transferred equip-
ment or supplies through service contracts or other
means, with or without reimbursement, as the Sec-
retary determines appropriate.

(6) REIMBURSEMENT OF EXPENSES.—The Sec-
retary of Homeland Security is authorized to collect
payment from the recipient government for the pro-
vision of training, shipping costs, supporting mate-
rials, maintenance, supplies, or other assistance in
support of provided equipment or supplies under this
subsection.

(7) RECEIPTS CREDITED AS OFFSETTING COL-
LECTIONS.—Notwithstanding section 3302 of title
31, United States Code, any amount collected under
this subsection—

(A) shall be credited as offsetting collec-
tions, subject to appropriations, to the account
that finances the activities and services for
which the payment is received; and

(B) shall remain available until expended
for the purpose of providing for the security in-
terests of the homeland.

(8) RULE OF CONSTRUCTION.—Nothing in this
subsection may be construed as affecting, aug-
menting, or diminishing the authority of the Secretary of State.

(9) DEFINITION.—For the purposes of this section, the term “excess nonlethal equipment and supplies” means equipment and supplies the Secretary of Homeland Security has determined is either not required for United States domestic operations, or would be more effective to homeland security if deployed for use outside of the United States.

(c) NOTIFICATION TO CONGRESS.—

(1) IN GENERAL.—Not later than 15 days before providing any systems or equipment or supplies under this section, the Secretary of Homeland Security and Secretary of State shall provide notification to the appropriate congressional committees of such provision.

(2) CONTENTS.—A notification required under paragraph (1) shall include the following:

(A) The specific vulnerability that will be mitigated by the provision of any systems or equipment or supplies under this section.

(B) An explanation as to why the recipient is unable or unwilling to independently acquire such systems or equipment or supplies.
(C) An evacuation plan for any sensitive
technologies in case of emergency or instability
in the country to which such systems or equip-
ment or supplies is being provided.

(D) How the United States Government
will ensure that such systems or equipment or
supplies are being maintained appropriately and
used as intended.

(E) The total dollar value of such systems,
equipment, and supplies.

(d) RULE OF CONSTRUCTION.—

(1) IN GENERAL.—The authority provided
under this section shall be exercised in accordance
with applicable provisions of the Arms Export Con-
trol Act (22 U.S.C. 2751 et seq.), the Export Ad-
ministration Regulations, or any other similar provi-
sion of law.

(2) DEFINITION.—In this subsection, the term
“Export Administration Regulations” means—

(A) the Export Administration Regulations
as maintained and amended under the authority
of the International Emergency Economic Pow-
ers Act (50 U.S.C. 1701 et seq.) and codified
in subchapter C of chapter VII of title 15, Code
of Federal Regulations; or
(B) any successor regulations.

SEC. 2603. ACTIONS WITH RESPECT TO FOREIGN COUNTRIES THAT FAIL TO MEET MINIMUM STANDARDS FOR SERIOUS AND SUSTAINED EFFORTS TO COMBAT TERRORIST AND FOREIGN FIGHTER TRAVEL.

(a) Reports to Congress.—

(1) In general.—Not later than April 30 of each year through 2021, the Secretary of State, in coordination with the Secretary of Homeland Security, shall submit to the appropriate congressional committees a report with respect to the status of efforts of foreign governments to combat terrorist and foreign fighter travel. The report shall include the following:

(A) A list of those foreign countries, if any, to which the minimum standards for serious and sustained efforts to combat terrorist and foreign fighter travel as described in subsection (b) are applicable and whose governments comply with such standards.

(B) A list of those foreign countries, if any, to which the minimum standards for serious and sustained efforts to combat terrorist and fighter travel as described in subsection (b)
are applicable and whose governments do not yet fully comply with such standards but are making significant efforts to bring themselves into compliance.

(C) A list of those foreign countries, if any, to which the minimum standards for serious and sustained efforts to combat terrorist and foreign fighter travel as described in subsection (b) are applicable and whose governments do not fully comply with such standards and are not making significant efforts to bring themselves into compliance.

(D) A description for each foreign country identified in subparagraphs (B) and (C) of the areas in which the government of the foreign country does not meet the minimum standards for serious and sustained efforts to combat terrorist and foreign fighter travel as described in subsection (b).

(2) Form.—The report required by paragraph (1) shall be submitted in unclassified form, but may contain a classified annex, if necessary.

(3) Inclusion in Country Reports on Terrorism.—To the maximum extent practicable, the Secretary of State, in coordination with the Sec-

(b) Minimum Standards Described.—The minimum standards for serious and sustained efforts to combat terrorist and foreign fighter travel applicable to the government of a foreign country are the following:

(1) The government of the country makes meaningful efforts to identify and monitor terrorists and foreign fighters operating within the territory of the country.

(2) The government of the country regularly exchanges substantive counterterrorism information with other foreign governments, including the United States Government, through bilateral or multilateral channels and international organizations such as INTERPOL, and cooperates with other foreign governments in the investigation and prosecution of terrorists and foreign fighters.

(3) The government of the country implements effective border controls or participates in an existing border-crossing control regime that has been de-
terminated by the United States Government to em-
ploy effective border-crossing oversight.

(4) The government of the country has controls
and systems in place to prevent and report upon
counterfeiting, forgery, and fraudulent use or pos-
session of false, stolen, or lost identity papers and
travel documents.

(5) The government of the country collects air
passenger data and employs evidence-based traveler
risk assessment and screening procedures, including
collection and analysis of travel data.

(6) The government of the country appro-
priately screens travelers, including vetting of trav-
elers at air, sea, and land ports of entry, against
counterterrorism and other criminal databases, as
appropriate.

(7) The government of the country submits in-
formation to INTERPOL databases and screens
travelers against INTERPOL databases at ports of
entry and exit.

(8) The government of the country has estab-
lished and implemented domestic laws criminalizing
material support to foreign terrorist organizations
and has the ability and willingness to prosecute
cases involving such material support to foreign terrorist organizations.

(9) The government of the country takes measures to prevent individuals in its territory from traveling abroad to enlist with or provide material support to foreign terrorist organizations.

(10) The government of the country takes measures to ensure a minimal level of corruption and likelihood that corruption could impact the veracity of security and intelligence reporting from the country, a minimal likelihood that such corruption could adversely affect the legitimacy of national identity papers of the country, and the country does not shelter suspects from investigation and prosecution.

(11) The government of a country is not determined to be a high-risk program country under section 217(c)(12) of the Immigration and Nationality Act (8. U.S.C. 1187(c)(12)).

(e) SUSPENSION OF ASSISTANCE.—The Secretary of State, in consultation with the Secretary of Homeland Security and the heads of other Federal agencies, as appropriate, is authorized to suspend nonhumanitarian, nontrade-related foreign assistance to any government of a foreign country if the foreign country is identified in
subparagraph (C) of subsection (a)(1) in the most recent
report submitted to the appropriate congressional commit-
tees under such subsection.

SEC. 2604. DEFINITIONS.

In this title:

(1) APPROPRIATE CONGRESSIONAL COMMIT-
TEES.—The term "appropriate congressional com-
mittees" means the Committee on Homeland Secu-
rit y and Governmental Affairs, the Committee on
Foreign Relations, the Committee on the Judiciary,
and the Committee on Commerce, Science, and
Transportation of the Senate and the Committee on
Homeland Security, the Committee on the Judiciary,
and the Committee on Foreign Affairs of the House
of Representatives.

(2) FOREIGN TERRORIST ORGANIZATION.—The
term "foreign terrorist organization" means an or-
ganization that is designated as a foreign terrorist
organization pursuant to section 219 of the Immi-

(3) NONHUMANITARIAN, NONTRADE-RELATED
FOREIGN ASSISTANCE.—The term "nonhumani-
tarian, nontrade-related foreign assistance" has the
meaning given the term in section 103 of the Traf-

SEC. 2605. PROHIBITION ON ADDITIONAL FUNDING.

No additional funds are authorized to be appropriated to carry out this title.

TITLE XXVII—SOUTHWEST BORDER SECURITY THREAT ASSESSMENT

SEC. 2701. SOUTHWEST BORDER THREAT ANALYSIS.

(a) In General.—Not later than 180 days after the date of the enactment of this Act, the Secretary of Homeland Security shall submit to the Committee on Homeland Security of the House of Representatives and the Committee on Homeland Security and Governmental Affairs of the Senate a southwest border threat analysis that includes the following:

(1) An assessment of current and potential terrorism and criminal threats posed by individuals and organized groups seeking to—

(A) unlawfully enter the United States through the southwest border; or

(B) exploit security vulnerabilities along the southwest border.

(2) An assessment of improvements needed at and between ports of entry along the southwest bor-
der to prevent terrorists and instruments of terror from entering the United States.

(3) An assessment of gaps in law, policy, and coordination between State, local, or tribal law enforcement, international agreements, or tribal agreements that hinder effective and efficient border security, counterterrorism, and anti-human smuggling and trafficking efforts.

(4) An assessment of the flow of legitimate trade along the southwest border.

(5) An assessment of the current percentage of situational awareness achieved by the Department of Homeland Security along the southwest border.

(6) An assessment of the current percentage of operational control (as such term is defined in section 2 of the Secure Fence Act of 2006 (8 U.S.C. 1701 note; Public Law 109–367)) achieved by the Department of Homeland Security of the southwest.

(7) An assessment of impact of trusted traveler programs on border wait times and border security.

(8) An assessment of traveler crossing times and any potential security vulnerability associated with prolonged wait times.

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

(1) Technology needs and challenges, including such needs and challenges identified as a result of previous investments that have not fully realized the security and operational benefits that were sought.

(2) Personnel needs and challenges, including such needs and challenges associated with recruitment and hiring.

(3) Infrastructure needs and challenges.

(4) The roles and authorities of State, local, and tribal law enforcement in general border security activities.

(5) The status of coordination among Federal, State, local, tribal, and Mexican law enforcement entities relating to border security.

(6) The terrain, population density, and climate along the southwest border.

(7) International agreements between the United States and Mexico related to border security.

(c) CLASSIFIED THREAT ANALYSIS.—To the extent possible, the Secretary of Homeland Security shall submit the southwest border threat analysis required under subsection (a) in unclassified form. The Secretary may submit
a portion of such threat analysis in classified form if the
Secretary determines such is appropriate.

SEC. 2702. BORDER PATROL STRATEGIC PLAN.

(a) IN GENERAL.—Not later than 180 days after the
submission of the threat analysis required under section
2701 but not later than June 30, 2017, and every five
years thereafter, the Secretary of Homeland Security, act-
ing through the Chief of U.S. Border Patrol, shall, in con-
sultation with the Officer for Civil Rights and Civil Lib-
erties of the Department of Homeland Security, issue a
Border Patrol Strategic Plan.

(b) CONTENTS.—The Border Patrol Strategic Plan
required under subsection (a) shall include, at a minimum,
a consideration of the following:

(1) The southwest border threat analysis re-
quired under section 2701, with an emphasis on ef-
forts to mitigate threats identified in such threat
analysis.

(2) Efforts to analyze and disseminate border
security and border threat information between De-
partment of Homeland Security border security com-
ponents and with other appropriate Federal depart-
ments and agencies with missions associated with
the border.
(3) Efforts to increase situational awareness, including the following:

(A) Surveillance capabilities, including capabilities developed or utilized by the Department of Defense, and any appropriate technology determined to be excess by the Department of Defense.

(B) Use of manned aircraft and unmanned aerial systems, including camera and sensor technology deployed on such assets.

(4) Efforts to detect and prevent terrorists and instruments of terrorism from entering the United States.

(5) Efforts to detect, interdict, and disrupt aliens and illicit drugs at the earliest possible point.

(6) Efforts to focus intelligence collection to disrupt transnational criminal organizations outside of the international and maritime borders of the United States.

(7) Efforts to ensure that any new border security technology can be operationally integrated with existing technologies in use by the Department of Homeland Security.

(8) Technology required to maintain, support, and enhance security and facilitate trade at ports of
entry, including nonintrusive detection equipment, radiation detection equipment, biometric technology, surveillance systems, and other sensors and technology that the Secretary of Homeland Security determines necessary.

(9) Operational coordination unity of effort initiatives of the border security components of the Department of Homeland Security, including any relevant task forces of the Department.

(10) Lessons learned from Operation Jumpstart and Operation Phalanx.

(11) Cooperative agreements and information sharing with State, local, tribal, territorial, and other Federal law enforcement agencies that have jurisdiction on the northern or southern border.

(12) Border security information received from consultation with State, local, tribal, territorial, and Federal law enforcement agencies that have jurisdiction on the northern or southern border, or in the maritime environment, and from border community stakeholders (including through public meetings with such stakeholders), including representatives from border agricultural and ranching organizations and representatives from business and civic organizations along the northern or southern border.
(13) Staffing requirements for all departmental border security functions.

(14) A prioritized list of departmental research and development objectives to enhance the security of the southwest border.

(15) An assessment of training programs, including training programs regarding the following:

(A) Identifying and detecting fraudulent documents.

(B) Understanding the scope of enforcement authorities and the use of force policies.

(C) Screening, identifying, and addressing vulnerable populations, such as children and victims of human trafficking.

(16) An assessment of how border security operations affect crossing times.

SEC. 2703. DEFINITIONS.

In this title:

(1) Situational awareness.—The term “situational awareness” means a knowledge and unified understanding of unlawful cross-border activity, including threats and trends concerning illicit trafficking and unlawful crossings (which may be used to forecast future shifts in such threats and trends), and the operational capability to conduct continuous
and integrated surveillance of the international borders of the United States.

(2) Southwest Border.—The term "southwest border" means the land and maritime borders between the United States and Mexico.

**TITLE XXVIII—NATIONAL STRATEGY TO COMBAT TERRORIST TRAVEL**

**(a) Sense of Congress.—**It is the sense of Congress that it should be the policy of the United States to—

(1) continue to regularly assess the evolving terrorist threat to the United States;

(2) catalogue existing Federal Government efforts to obstruct terrorist and foreign fighter travel into, out of, and within the United States, as well as overseas;

(3) identify such efforts that may benefit from reform or consolidation, or require elimination;

(4) identify potential security vulnerabilities in United States defenses against terrorist travel; and

(5) prioritize resources to address in a risk-based manner any such security vulnerabilities.

**(b) National Strategy and Updates.—**
(1) IN GENERAL.—In accordance with paragraph (2), the President shall transmit to the appropriate congressional committees a national strategy (including, as appropriate, updates to such strategy) to combat terrorist travel. The strategy shall address efforts to intercept terrorists and foreign fighters and constrain the domestic and international travel of such persons. Consistent with the protection of classified information, the strategy shall be submitted in unclassified form, including, as appropriate, a classified annex.

(2) TIMING.—

(A) INITIAL STRATEGY.—The initial national strategy required under paragraph (1) shall be transmitted not later than 180 days after the date of the enactment of this Act.

(B) UPDATED STRATEGIES.—Updated national strategies under paragraph (1) shall be transmitted not later than 180 days after the commencement of a new Presidential administration.

(3) COORDINATION.—The President shall direct the Secretary of Homeland Security to develop the initial national strategy and updates required under this subsection and shall direct, as appropriate, the
head of other Federal agencies to coordinate with
the Secretary in the development of such strategy
and updates.

(4) CONTENTS.—The initial national strategy
and updates required under this subsection shall—

(A) include an accounting and description
of all Federal Government programs, projects,
and activities to constrain domestic and inter-
national travel by terrorists and foreign fight-
ers;

(B) identify specific security vulnerabilities
within the United States and abroad that may
be exploited by terrorists and foreign fighters;

(C) delineate goals for—

(i) closing the security vulnerabilities
identified in accordance with subparagraph
(B); and

(ii) enhancing the Federal Govern-
ment’s ability to constrain domestic and
international travel by terrorists and for-
eign fighters; and

(D) describe actions to be taken to achieve
the goals delineated in subparagraph (C), as
well as the means needed to do so, including—
(i) steps to reform, improve, and streamline existing Federal Government efforts to align with the current threat environment;

(ii) new programs, projects, or activities that are requested, under development, or undergoing implementation;

(iii) new authorities or changes in existing authorities needed from Congress;

(iv) specific budget adjustments being requested to enhance United States security in a risk-based manner; and

(v) an identification of Federal departments and agencies responsible for specific actions described in this subparagraph.

(5) SUNSET.—The requirement to transmit updated national strategies under this subsection shall terminate on the date that is 7 years after the date of the enactment of this Act.

(c) DEVELOPMENT OF IMPLEMENTATION PLANS.—For each national strategy required under subsection (b), the President shall direct the Secretary of Homeland Security to develop an implementation plan for the Department of Homeland Security and coordinate with the heads
of other relevant Federal agencies to ensure the development of implementing plans for each such agency.

(d) IMPLEMENTATION PLANS.—

(1) IN GENERAL.—The President shall transmit to the appropriate congressional committees implementation plans for each national strategy required under subsection (b). Consistent with the protection of classified information, each such implementation plan shall be transmitted in unclassified form, but may include a classified annex.

(2) TIMING.—The implementation plans referred to in paragraph (1) shall be transmitted simultaneously with each national strategy required under subsection (b). Such implementation plans shall be updated and transmitted to the appropriate congressional committees on an annual basis.

(3) SUNSET.—The requirement to transmit implementation plans under paragraph (1) shall terminate on the date that is 10 years after the date of the enactment of this Act.

(e) PROHIBITION ON ADDITIONAL FUNDING.—No additional funds are authorized to be appropriated to carry out this section.

(f) DEFINITION.—In this section, the term “appropriate congressional committees” means—
(1) in the House of Representatives—
   (A) the Committee on Homeland Security;
   (B) the Committee on Armed Services;
   (C) the Permanent Select Committee on Intelligence;
   (D) the Committee on the Judiciary;
   (E) the Committee on Foreign Affairs; and
   (F) the Committee on Appropriations; and

(2) in the Senate—
   (A) the Committee on Homeland Security and Governmental Affairs;
   (B) the Committee on Armed Services;
   (C) the Select Committee on Intelligence;
   (D) the Committee on the Judiciary;
   (E) the Committee on Foreign Relations;

   and

   (F) the Committee on Appropriations.

TITLE XXIX—STATE AND HIGH-RISK URBAN AREA WORKING GROUP

SEC. 2901. ADMINISTRATION AND COORDINATION OF CERTAIN DHS GRANTS.

Subsection (b) of section 2021 of the Homeland Security Act of 2002 (6 U.S.C. 611) is amended to read as follows:
“(b) Planning Committees.—

“(1) In general.—Any State or high-risk urban area receiving a grant under section 2003 or 2004 shall establish a State planning committee or urban area working group to assist in preparation and revision of the State, regional, or local homeland security plan or the threat and hazard identification and risk assessment, as the case may be, and to assist in determining effective funding priorities for grants under such sections.

“(2) Composition.—

“(A) In general.—The State planning committees and urban area working groups referred to in paragraph (1) shall include at least one representative from each of the following significant stakeholders:

“(i) Local or tribal government officials.

“(ii) Emergency response providers, which shall include representatives of the fire service, law enforcement, emergency medical services, and emergency managers.

“(iii) Public health officials and other appropriate medical practitioners.
“(iv) Individuals representing educational institutions, including elementary schools, community colleges, and other institutions of higher education.

“(v) State and regional interoperable communications coordinators, as appropriate.

“(vi) State and major urban area fusion centers, as appropriate.

“(B) Geographic Representation.—

The members of the State planning committee or urban area working group, as the case may be, shall be a representative group of individuals from the counties, cities, towns, and Indian tribes within the State or high-risk urban area, including, as appropriate, representatives of rural, high-population, and high-threat jurisdictions.

“(3) Existing Planning Committees.—Nothing in this subsection may be construed to require that any State or high-risk urban area create a State planning committee or urban area working group, as the case may be, if that State or high-risk urban area has established and uses a multijuris-
dictional planning committee or commission that meets the requirements of this subsection.”.

**TITLE XXX—STATE AND LOCAL CYBER PROTECTION**

**SEC. 3001. STATE AND LOCAL COORDINATION ON CYBERSECURITY WITH THE NATIONAL CYBERSECURITY AND COMMUNICATIONS INTEGRATION CENTER.**

(a) In general.—The second section 226 of the Homeland Security Act of 2002 (6 U.S.C. 148; relating to the national cybersecurity and communications integration center) is amended by adding at the end the following new subsection:

“(g) State and Local Coordination on Cybersecurity.—

“(1) In general.—The Center shall, to the extent practicable—

“(A) assist State and local governments, upon request, in identifying information system vulnerabilities;

“(B) assist State and local governments, upon request, in identifying information security protections commensurate with cybersecurity risks and the magnitude of the potential harm resulting from the unauthorized access,
use, disclosure, disruption, modification, or de-
struction of—

“(i) information collected or main-
tained by or on behalf of a State or local
government; or

“(ii) information systems used or op-
erated by an agency or by a contractor of
a State or local government or other orga-
nization on behalf of a State or local gov-
ernment;

“(C) in consultation with State and local
governments, provide and periodically update
via a web portal tools, products, resources, poli-
cies, guidelines, and procedures related to infor-
mation security;

“(D) work with senior State and local gov-
ernment officials, including State and local
Chief Information Officers, through national as-
associations to coordinate a nationwide effort to
ensure effective implementation of tools, prod-
ucts, resources, policies, guidelines, and proce-
dures related to information security to secure
and ensure the resiliency of State and local in-
formation systems;
“(E) provide, upon request, operational and technical cybersecurity training to State and local government and fusion center analysts and operators to address cybersecurity risks or incidents;

“(F) provide, in coordination with the Chief Privacy Officer and the Chief Civil Rights and Civil Liberties Officer of the Department, privacy and civil liberties training to State and local governments related to cybersecurity;

“(G) provide, upon request, operational and technical assistance to State and local governments to implement tools, products, resources, policies, guidelines, and procedures on information security by—

“(i) deploying technology to assist such State or local government to continuously diagnose and mitigate against cyber threats and vulnerabilities, with or without reimbursement;

“(ii) compiling and analyzing data on State and local information security; and

“(iii) developing and conducting targeted operational evaluations, including threat and vulnerability assessments, on
the information systems of State and local governments;

“(H) assist State and local governments to develop policies and procedures for coordinating vulnerability disclosures, to the extent practicable, consistent with international and national standards in the information technology industry, including standards developed by the National Institute of Standards and Technology; and

“(I) ensure that State and local governments, as appropriate, are made aware of the tools, products, resources, policies, guidelines, and procedures on information security developed by the Department and other appropriate Federal departments and agencies for ensuring the security and resiliency of Federal civilian information systems.

“(2) TRAINING.—Privacy and civil liberties training provided pursuant to subparagraph (F) of paragraph (1) shall include processes, methods, and information that—

“(A) are consistent with the Department’s Fair Information Practice Principles developed pursuant to section 552a of title 5, United
States Code (commonly referred to as the ‘Privacy Act of 1974’ or the ‘Privacy Act’);

“(B) reasonably limit, to the greatest extent practicable, the receipt, retention, use, and disclosure of information related to cybersecurity risks and incidents associated with specific persons that is not necessary, for cybersecurity purposes, to protect an information system or network of information systems from cybersecurity risks or to mitigate cybersecurity risks and incidents in a timely manner;

“(C) minimize any impact on privacy and civil liberties;

“(D) provide data integrity through the prompt removal and destruction of obsolete or erroneous names and personal information that is unrelated to the cybersecurity risk or incident information shared and retained by the Center in accordance with this section;

“(E) include requirements to safeguard cyber threat indicators and defensive measures retained by the Center, including information that is proprietary or business-sensitive that may be used to identify specific persons from unauthorized access or acquisition;
“(F) protect the confidentiality of cyber threat indicators and defensive measures associated with specific persons to the greatest extent practicable; and

“(G) ensure all relevant constitutional, legal, and privacy protections are observed.”.

(b) CONGRESSIONAL OVERSIGHT.—Not later than 2 years after the date of the enactment of this Act, the national cybersecurity and communications integration center of the Department of Homeland Security shall provide to the Committee on Homeland Security of the House of Representatives and the Committee on Homeland Security and Governmental Affairs of the Senate information on the activities and effectiveness of such activities under subsection (g) of the second section 226 of the Homeland Security Act of 2002 (6 U.S.C. 148; relating to the national cybersecurity and communications integration center), as added by subsection (a) of this section, on State and local information security. The center shall seek feedback from State and local governments regarding the effectiveness of such activities and include such feedback in the information required to be provided under this subsection.
TITLE XXXI—FUSION CENTER
ENHANCEMENT

SEC. 3101. DEPARTMENT OF HOMELAND SECURITY FUSION
CENTER PARTNERSHIP INITIATIVE.

(a) IN GENERAL.—Section 210A of the Homeland
Security Act of 2002 (6 U.S.C. 124h) is amended—
(1) by amending the section heading to read as
follows:
“SEC. 210A. DEPARTMENT OF HOMELAND SECURITY FU-
SION CENTER PARTNERSHIP INITIATIVE.”;
(2) in subsection (a), by adding at the end the
following new sentence: “Beginning on the date of
the enactment of the Fusion Center Enhancement
Act of 2015, such Initiative shall be known as the
‘Department of Homeland Security Fusion Center
Partnership Initiative’.”;
(3) by amending subsection (b) to read as fol-
lows:
“(b) INTERAGENCY SUPPORT AND COORDINATION.—
Through the Department of Homeland Security Fusion
Center Partnership Initiative, in coordination with prin-
cipal officials of fusion centers in the National Network
of Fusion Centers and the officers designated as the
Homeland Security Advisors of the States, the Secretary
shall—
“(1) coordinate with the heads of other Federal departments and agencies to provide operational and intelligence advice and assistance to the National Network of Fusion Centers;

“(2) support the integration of fusion centers into the information sharing environment;

“(3) support the maturation and sustainment of the National Network of Fusion Centers;

“(4) reduce inefficiencies and maximize the effectiveness of Federal resource support to the National Network of Fusion Centers;

“(5) provide analytic and reporting advice and assistance to the National Network of Fusion Centers;

“(6) review information within the scope of the information sharing environment, including homeland security information, terrorism information, and weapons of mass destruction information, that is gathered by the National Network of Fusion Centers and incorporate such information, as appropriate, into the Department’s own such information;

“(7) provide for the effective dissemination of information within the scope of the information sharing environment to the National Network of Fusion Centers;
“(8) facilitate close communication and coordination between the National Network of Fusion Centers and the Department and other Federal departments and agencies;

“(9) provide the National Network of Fusion Centers with expertise on Department resources and operations;

“(10) coordinate the provision of training and technical assistance to the National Network of Fusion Centers and encourage such fusion centers to participate in terrorism threat-related exercises conducted by the Department;

“(11) ensure, to the greatest extent practicable, that support for the National Network of Fusion Centers is included as a national priority in applicable homeland security grant guidance;

“(12) ensure that each fusion center in the National Network of Fusion Centers has a privacy policy approved by the Chief Privacy Officer of the Department and a civil rights and civil liberties policy approved by the Officer for Civil Rights and Civil Liberties of the Department;

“(13) coordinate the nationwide suspicious activity report initiative to ensure information gath-
ered by the National Network of Fusion Centers is incorporated as appropriate;

“(14) lead Department efforts to ensure fusion centers in the National Network of Fusion Centers are the primary focal points for the sharing of homeland security information, terrorism information, and weapons of mass destruction information with State and local entities to the greatest extent practicable;

“(15) develop and disseminate best practices on the appropriate levels for staffing at fusion centers in the National Network of Fusion Centers of qualified representatives from State, local, tribal, and territorial law enforcement, fire, emergency medical, and emergency management services, and public health disciplines, as well as the private sector; and

“(16) carry out such other duties as the Secretary determines appropriate.”;

(4) in subsection (e)—

(A) by striking so much as precedes paragraph (3)(B) and inserting the following:

“(c) Resource Allocation.—

“(1) Information Sharing and Personnel Assignment.—
“(A) INFORMATION SHARING.—The Under Secretary for Intelligence and Analysis shall ensure that, as appropriate—

“(i) fusion centers in the National Network of Fusion Centers have access to homeland security information sharing systems; and

“(ii) Department personnel are deployed to support fusion centers in the National Network of Fusion Centers in a manner consistent with the Department’s mission and existing statutory limits.

“(B) PERSONNEL ASSIGNMENT.—Department personnel referred to in subparagraph (A)(ii) may include the following:

“(i) Intelligence officers.

“(ii) Intelligence analysts.

“(iii) Other liaisons from components and offices of the Department, as appropriate.

“(C) MEMORANDA OF UNDERSTANDING.—The Under Secretary for Intelligence and Analysis shall negotiate memoranda of understanding between the Department and a State or local government, in coordination with the
appropriate representatives from fusion centers
in the National Network of Fusion Centers, re-
garding the exchange of information between
the Department and such fusion centers. Such
memoranda shall include the following:

“(i) The categories of information to
be provided by each entity to the other en-
tity that are parties to any such memo-
randa.

“(ii) The contemplated uses of the ex-
changed information that is the subject of
any such memoranda.

“(iii) The procedures for developing
joint products.

“(iv) The information sharing dispute
resolution processes.

“(v) Any protections necessary to en-
sure the exchange of information accords
with applicable law and policies.

“(2) SOURCES OF SUPPORT.—

“(A) IN GENERAL.—Information shared
and personnel assigned pursuant to paragraph
(1) may be shared or provided, as the case may
be, by the following Department components
and offices, in coordination with the respective
component or office head and in consultation with the principal officials of fusion centers in the National Network of Fusion Centers:

“(i) The Office of Intelligence and Analysis.

“(ii) The Office of Infrastructure Protection.

“(iii) The Transportation Security Administration.

“(iv) U.S. Customs and Border Protection.

“(v) U.S. Immigration and Customs Enforcement.

“(vi) The Coast Guard.

“(vii) Other components or offices of the Department, as determined by the Secretary.

“(B) COORDINATION WITH OTHER FEDERAL AGENCIES.—The Under Secretary for Intelligence and Analysis shall coordinate with appropriate officials throughout the Federal Government to ensure the deployment to fusion centers in the National Network of Fusion Centers of representatives with relevant expertise of other Federal departments and agencies.
“(3) Resource allocation criteria.—

“(A) In general.—The Secretary shall make available criteria for sharing information and deploying personnel to support a fusion center in the National Network of Fusion Centers in a manner consistent with the Department’s mission and existing statutory limits.”;

and

(B) in paragraph (4)(B), in the matter preceding clause (i), by inserting “in which such fusion center is located” after “region”;

(5) in subsection (d)—

(A) in paragraph (3), by striking “and” at the end;

(B) in paragraph (4)—

(i) by striking “government” and inserting “governments”; and

(ii) by striking the period at the end and inserting “; and”; and

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

“(5) utilize Department information, including information held by components and offices, to develop analysis focused on the mission of the Department under section 101(b).”;
(6) in subsection (e)—

(A) by amending paragraph (1) to read as follows:

“(1) IN GENERAL.—To the greatest extent practicable, the Secretary shall make it a priority to allocate resources, including deployed personnel, under this section from U.S. Customs and Border Protection, U.S. Immigration and Customs Enforcement, and the Coast Guard to support fusion centers in the National Network of Fusion Centers located in jurisdictions along land or maritime borders of the United States in order to enhance the integrity of and security at such borders by helping Federal, State, local, tribal, and territorial law enforcement authorities to identify, investigate, and otherwise interdict persons, weapons, and related contraband that pose a threat to homeland security.”; and

(B) in paragraph (2), in the matter preceding subparagraph (A), by striking “participating State, local, and regional”;

(7) in subsection (j)—

(A) in paragraph (4), by striking “and” at the end;

(B) by redesignating paragraph (5) as paragraph (6); and
(C) by inserting after paragraph (4) the following new paragraph:

“(5) the term ‘National Network of Fusion Centers’ means a decentralized arrangement of fusion centers intended to enhance individual State and urban area fusion centers’ ability to leverage the capabilities and expertise of all fusion centers for the purpose of enhancing analysis and homeland security information sharing nationally; and”;

(8) by striking subsection (k).

(b) ACCOUNTABILITY REPORT.—Not later than 1 year after the date of the enactment of this Act and annually thereafter through 2022, the Under Secretary for Intelligence and Analysis of the Department of Homeland Security shall report to the Committee on Homeland Security and the Permanent Select Committee on Intelligence of the House of Representatives and the Committee on Homeland Security and Governmental Affairs and the Select Committee on Intelligence of the Senate on the efforts of the Office of Intelligence and Analysis of the Department and other relevant components and offices of the Department to enhance support provided to fusion centers in the National Network of Fusion Centers, including meeting the requirements specified in section 210A of the
Homeland Security Act of 2002 (6 U.S.C. 124h), as amended by subsection (a) of this section.

(c) Clerical Amendment.—The table of contents in section 1(b) of such Act is amended by striking the item relating to section 210A and inserting the following new item:

“Sec. 210A. Department of Homeland Security Fusion Centers Initiative.”

(d) Reference.—Any reference in any law, rule, or regulation to the “Department of Homeland Security State, Local, and Regional Fusion Center Initiative” shall be deemed to be a reference to the “Department of Homeland Security Fusion Center Initiative”.

TITLE XXXII—TRANSPORTATION SECURITY ADMINISTRATION

REFORM AND IMPROVEMENT

SEC. 3201. DEFINITIONS.

In this title:

(1) Administration; TSA.—The terms “Administration” and “TSA” mean the Transportation Security Administration.

(2) Administrator.—The term “Administrator” means the Administrator of the Transportation Security Administration.

(3) Intelligence Community.—The term “intelligence community” has the meaning given
such term in section 3(4) of the National Security Act of 1947 (50 U.S.C. 3003(4)).

(4) DEPARTMENT.—The term “Department” means the Department of Homeland Security.

(5) SECURE FLIGHT.—The term “Secure Flight” means the Administration’s watchlist matching program.

Subtitle A—Aviation Security

SEC. 3211. TSA PRECHECK.

(a) TSA PreCheck.—Not later than 90 days after the date of the enactment of this Act, the Administrator shall—

(1) ensure that all screening of passengers and their accessible property shall be conducted in a risk-based, intelligence-driven manner with consideration given to the privacy and civil liberties of such passengers; and

(2) operate a trusted passenger screening program known as “TSA PreCheck” that provides expedited screening for low-risk passengers and their accessible property based on a comprehensive and continuous analysis of factors specified in subsection (b).

(b) FACTORS.—Factors referred to in subsection (a)(2) shall include the following:
(1) Whether passengers described in such subsection are members of other trusted traveler programs of the Department.

(2) Whether such passengers are traveling pursuant to subsection (m) of section 44903 of title 49, United States Code (as established under the Risk-Based Security for Members of the Armed Forces Act (Public Law 112–86)), section 44927 of such title (as established under the Helping Heroes Fly Act (Public Law 113–27)), or section 44928 of such title (as established under the Honor Flight Act (Public Law 113–221)).

(3) Whether such passengers possess an active security clearance or other credential issued by the Federal Government for which TSA has conducted a written threat assessment and determined that such passengers present a low risk to transportation or national security.

(4) Whether such passengers are members of a population for whom TSA has conducted a written security threat assessment, determined that such population poses a low risk to transportation or national security, and has issued such passengers a known traveler number.
(5) The ability of the Administration to verify such passengers’ identity and whether such passengers pose a risk to aviation security.

(6) Threats to transportation or national security as identified by the intelligence community and law enforcement community.

(e) ENROLLMENT EXPANSION.—

(1) IN GENERAL.—Not later than 90 days after the date of the enactment of this Act, the Administrator shall publish PreCheck application enrollment standards to add multiple private sector application capabilities for the TSA PreCheck program to increase the public’s enrollment access to such program, including standards that allow the use of secure technologies, including online enrollment, kiosks, tablets, or staffed computer stations at which individuals can apply for entry into such program.

(2) REQUIREMENTS.—Upon publication of the PreCheck program application enrollment standards pursuant to paragraph (1), the Administrator shall—

(A) coordinate with interested parties to deploy TSA-approved ready-to-market private sector solutions that meet the TSA PreCheck application enrollment standards described in
paragraph (1), make available additional
PreCheck enrollment capabilities, and offer se-
cure online and mobile enrollment opportuni-
ties;

(B) partner with the private sector to col-
lect biographic and biometric identification in-
formation via kiosks, mobile devices, or other
mobile enrollment platforms to reduce the num-
ber of instances in which passengers need to
travel to enrollment centers;

(C) ensure that the kiosks, mobile devices,
or other mobile enrollment platforms referred to
in subparagraph (E) are secure and not vulner-
able to data breaches;

(D) ensure that any biometric and bio-
graphic information is collected in a manner
which is comparable with the National Institute
of Standards and Technology standards and en-
sures privacy and data security protections, in-
cluding that applicants’ personally identifiable
information is collected, retained, used, and
shared in a manner consistent with section
552a of title 5, United States Code (commonly
known as the “Privacy Act of 1974”), and
agency regulations;
(E) ensure that an individual who wants to enroll in the PreCheck program and has started an application with a single identification verification at one location will be able to save such individual’s application on any kiosk, personal computer, mobile device, or other mobile enrollment platform and be able to return within a reasonable time to submit a second identification verification; and

(F) ensure that any enrollment expansion using a private sector risk assessment instead of a fingerprint-based criminal history records check is determined, by the Secretary of Homeland Security, to be equivalent to a fingerprint-based criminal history records check conducted through the Federal Bureau of Investigation.

(3) MARKETING OF PRECHECK PROGRAM.— Upon publication of PreCheck program application enrollment standards pursuant to paragraph (1), the Administrator shall—

(A) in accordance with such standards, develop and implement—

(i) a process, including an associated timeframe, for approving private sector
marketing of the TSA PreCheck program;
and

(ii) a strategy for partnering with the
private sector to encourage enrollment in
such program; and

(B) submit to Congress a report on any
PreCheck fees collected in excess of the costs of
administering such program, including rec-
ommendations for using such amounts to sup-
port marketing of such program under this sub-
section.

(4) IDENTIFICATION VERIFICATION ENHANCEMENT.—
Not later than 90 days after the date of the enact-
ment of this Act, the Administrator shall—

(A) coordinate with the heads of appro-
priate components of the Department to lever-
age Department-held data and technologies to
verify the citizenship of individuals enrolling in
the TSA PreCheck program; and

(B) partner with the private sector to use
advanced biometrics and standards comparable
with National Institute of Standards and Tech-
nology standards to facilitate enrollment in
such program.
(5) **Precheck lane operation.**—The Administrator shall—

(A) ensure that TSA PreCheck screening lanes are open and available during peak and high-volume travel times at airports to individuals enrolled in the PreCheck program; and

(B) make every practicable effort to provide expedited screening at standard screening lanes during times when PreCheck screening lanes are closed to individuals enrolled in such program in order to maintain operational efficiency.

(6) **Vetting for Precheck participants.**—Not later than 90 days after the date of the enactment of this Act, the Administrator shall initiate an assessment of the security vulnerabilities in the vetting process for the PreCheck program that includes an evaluation of whether subjecting PreCheck participants to recurrent fingerprint-based criminal history records checks, in addition to recurrent checks against the terrorist watchlist, could be done in a cost-effective manner to strengthen the security of the PreCheck program.
SEC. 3212. PRECHECK AND GENERAL PASSENGER BIOMETRIC IDENTIFICATION.

(a) In General.—Not later than 1 year after the date of enactment of this Act, the Administrator shall conduct a pilot project to establish a secure, automated, biometric-based system at airports to verify the identity of passengers who are members of TSA PreCheck. Such system shall—

(1) reduce the need for security screening personnel to perform travel document verification for individuals enrolled in TSA PreCheck;

(2) reduce the average wait time of individuals enrolled in TSA PreCheck;

(3) reduce overall operating expenses of the Administration;

(4) be integrated with the Administration’s watch list and trusted traveler matching program;

(5) be integrated with other checkpoint technologies to further facilitate risk-based passenger screening at the checkpoint, to the extent practicable and consistent with security standards; and

(6) consider capabilities and policies of U.S. Customs and Border Protection’s Global Entry Program, as appropriate.
(b) Establishment of Screening System for Certain Passengers.—Section 44901 of title 49, United States Code is amended—

(1) by redesignating subsections (c) through (l) as subsections (d) through (m), respectively; and

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

“(c) Establishment of Screening System for Certain Passengers.—Not later than December 31, 2017, in accordance with the requirements of the Transportation Security Administration Reform and Improvement Act of 2015, the Administrator of the Transportation Security Administration shall establish a secure, automated system at all large hub airports for verifying travel and identity documents of passengers who are not members of the Administration’s risk-based aviation passenger screening program, known as ‘TSA PreCheck’. Such system shall—

“(1) assess the need for security screening personnel to perform travel document verification for such passengers, thereby assessing the overall number of such screening personnel;

“(2) assess the average wait time of such passengers;
“(3) assess overall operating expenses of the Administration;

“(4) be integrated with the Administration’s watch list matching program; and

“(5) be integrated with other checkpoint technologies to further facilitate risk-based passenger screening at the checkpoint, to the extent practicable and consistent with security standards.”.

SEC. 3213. LIMITATION; PRECHECK OPERATIONS MAINTAINED; ALTERNATE METHODS.

(a) In General.—Except as provided in subsection (c), the Administrator shall direct that access to expedited airport security screening at an airport security checkpoint be limited to only the following:

(1) A passenger who voluntarily submits biographic and biometric information for a security risk assessment and whose application for the PreCheck program has been approved, or a passenger who is a participant in another trusted or registered traveler program of the Department.

(2) A passenger traveling pursuant to section 44903 of title 49, United States Code (as established under the Risk-Based Security for Members of the Armed Forces Act (Public Law 112–86)), section 44927 of such title (as established under the
Helping Heroes Fly Act (Public Law 113–27)), or
section 44928 of such title (as established under the
Honor Flight Act (Public Law 113–221)).

(3) A passenger who did not voluntarily submit
biographic and biometric information for a security
risk assessment but is a member of a population
designated by the Administrator as known and low-
risk and who may be issued a unique, known travel-
er number by the Administrator determining that
such passenger is a member of a category of travel-
ers designated by the Administrator as known and
low-risk.

(b) PreCheck Operations Maintained.—In car-
rying out subsection (a), the Administrator shall ensure
that expedited airport security screening remains available
to passengers at or above the level that exists on the day
before the date of the enactment of this Act.

(c) Frequent Fliers.—If the Administrator deter-
mines that such is appropriate, the implementation of sub-
section (a) may be delayed by up to 1 year with respect
to the population of passengers who did not voluntarily
submit biographic and biometric information for security
risk assessments but who nevertheless receive expedited
airport security screening because such passengers are
designated as frequent fliers by air carriers. If the Admin-
istrator uses the authority provided by this subsection, the
Administrator shall notify the Committee on Homeland
Security of the House of Representatives and the Com-
mittee on Homeland Security and Governmental Affairs
and the Committee on Commerce, Science, and Transpor-
tation of the Senate of such phased-in implementation.

(d) ALTERNATE METHODS.—The Administrator may
provide access to expedited airport security screening to
additional passengers pursuant to an alternate method
upon the submission to the Committee on Homeland Secu-
rity of the House of Representatives and the Committee
on Commerce, Science, and Transportation of the Senate
of an independent assessment of the security effectiveness
of such alternate method that is conducted by an inde-
pendent entity that determines that such alternate method
is designed to—

(1) reliably and effectively identify passengers
who likely pose a low risk to the United States avia-
tion system;

(2) mitigate the likelihood that a passenger who
may pose a security threat to the United States
aviation system is selected for expedited security
screening; and

(3) address known and evolving security risks
to the United States aviation system.
(e) INFORMATION SHARING.—The Administrator shall provide to the entity conducting the independent assessment under subsection (d) effectiveness testing results that are consistent with established evaluation design practices, as identified by the Comptroller General of the United States.

(f) REPORTING.—Not later than 3 months after the date of the enactment of this Act and annually thereafter, the Administrator shall report to the Committee on Homeland Security of the House of Representatives and the Committee on Commerce, Science, and Transportation of the Senate on the percentage of all passengers who are provided expedited security screening, and of such passengers so provided, the percentage who are participants in the PreCheck program (who have voluntarily submitted biographic and biometric information for security risk assessments), the percentage who are participants in another trusted traveler program of the Department, the percentage who are participants in the PreCheck program due to the Administrator’s issuance of known traveler numbers, and for the remaining percentage of passengers granted access to expedited security screening in PreCheck security lanes, information on the percentages attributable to each alternative method utilized by the Ad-
ministration to direct passengers to expedited airport se-
curity screening at PreCheck security lanes.

(g) RULE OF CONSTRUCTION.—Nothing in this sec-
tion may be construed to—

(1) authorize or direct the Administrator to re-
duce or limit the availability of expedited security
screening at an airport; or

(2) limit the authority of the Administrator to
use technologies and systems, including passenger
screening canines and explosives trace detection, as
a part of security screening operations.

SEC. 3214. SECURE FLIGHT PROGRAM.

Not later than 90 days after the date of the enact-
ment of this Act, the Administrator shall—

(1) develop a process for regularly evaluating
the root causes of screening errors at checkpoints
across airports so that corrective measures are able
to be identified;

(2) implement such corrective measures to ad-
dress the root causes of such screening errors occurring at the checkpoint;

(3) develop additional measures to address key
performance aspects related to the Secure Flight
program goals and ensure that such measures clear-
ly identify activities necessary to achieve progress to-
wards such goals;

(4) develop a mechanism to systematically docu-
ment the number and causes of Secure Flight pro-
gram matching errors for the purpose of improving
program performance and provide program man-
agers with timely and reliable information;

(5) provide job-specific privacy refresher train-
ing for Secure Flight program staff to further pro-
tect personally identifiable information in the Secure
Flight system program; and

(6) develop a mechanism to comprehensively
document and track key Secure Flight program pri-
vacy issues and decisions to ensure the Secure
Flight program has complete information for effec-
tive oversight of its privacy controls.

SEC. 3215. EFFICIENCY REVIEW BY TSA.

(a) Review Required.—Not later than 270 days
after the date of the enactment of this Act, the Adminis-
trator shall conduct and complete a comprehensive, agen-
cy-wide efficiency review of the Administration to identify
spending reductions and administrative savings through
the streamlining and any necessary restructuring of agen-
cy divisions to make the Administration more efficient. In
carrying out the review under this section, the Administrator shall consider each of the following:

(1) The elimination of any duplicative or overlapping programs and initiatives that can be streamlined.

(2) The elimination of any unnecessary or obsolete rules, regulations, directives, or procedures.

(3) Any other matters the Administrator determines are appropriate.

(b) REPORT TO CONGRESS.—Not later than 30 days after the completion of the efficiency review required under subsection (a), the Administrator shall submit to the Committee on Homeland Security of the House of Representatives and the Committee on Homeland Security and Governmental Affairs and the Committee on Commerce, Science, and Transportation of the Senate a report that specifies the results and cost savings expected to be achieved through such efficiency review. Such report shall also include information relating to how the Administration may use efficiencies identified through such efficiency review to provide funding to reimburse airports that incurred eligible costs for in-line baggage screening systems.
SEC. 3216. DONATION OF SCREENING EQUIPMENT TO PROTECT THE UNITED STATES.

(a) In general.—The Administrator is authorized to donate security screening equipment to a foreign last-point-of-departure airport operator if such equipment can be reasonably expected to mitigate a specific vulnerability to the security of the United States or United States citizens.

(b) Report to Congress.—Not later than 30 days before any donation of equipment under this section, the Administrator shall provide to the Committee on Homeland Security of the House of Representatives and the Committee on Homeland Security and Governmental Affairs and the Committee on Commerce, Science, and Transportation of the Senate a detailed written explanation of—

(1) the specific vulnerability to the United States that will be mitigated with such donation;

(2) an explanation as to why the recipient is unable or unwilling to purchase equipment to mitigate such threat;

(3) an evacuation plan for sensitive technologies in case of emergency or instability in the country to which such donation is being made;

(4) how the Administration will ensure the equipment that is being donated is used and main-
(5) the total dollar value of such donation.

SEC. 3217. REVIEW OF SUSTAINED SECURITY DIRECTIVES.

(a) In General.—Not later than 90 days after the date of the enactment of this Act and annually thereafter, for any security directive that has been in effect for longer than 1 year, the Administrator shall review the necessity of such directives, from a risk-based perspective.

(b) Briefing to Congress.—Upon completion of each review pursuant to subsection (a), the Administrator shall brief the Committee on Homeland Security of the House of Representatives and the Committee on Homeland Security and Governmental Affairs and the Committee on Commerce, Science, and Transportation of the Senate on—

(1) any changes being made to existing security directives as a result of each such review;

(2) the specific threat that is being mitigated by any such directive that will remain in effect; and

(3) the planned disposition of any such directive.
SEC. 3218. MAINTENANCE OF SECURITY-RELATED TECHNOLOGY.

(a) In General.—Title XVI of the Homeland Security Act of 2002 (6 U.S.C. 561 et seq.) is amended by adding at the end the following:

“Subtitle C—Maintenance of Security-Related Technology

“SEC. 1621. MAINTENANCE VALIDATION AND OVERSIGHT.

“(a) In General.—Not later than 180 days after the date of the enactment of this subtitle, the Administrator shall develop and implement a preventive maintenance validation process for security-related technology deployed to airports.

“(b) Maintenance by Administration Personnel at Airports.—For maintenance to be carried out by Administration personnel at airports, the process referred to in subsection (a) shall include the following:

“(1) Guidance to Administration personnel, equipment maintenance technicians, and other personnel at airports specifying how to conduct and document preventive maintenance actions.

“(2) Mechanisms for the Administrator to verify compliance with the guidance issued pursuant to paragraph (1).

“(c) Maintenance by Contractors at Airports.—For maintenance to be carried out by a con-
tractor at airports, the process referred to in subsection (a) shall require the following:

“(1) Provision of monthly preventive maintenance schedules to appropriate Administration personnel at each airport that includes information on each action to be completed by a contractor.

“(2) Notification to appropriate Administration personnel at each airport when maintenance action is completed by a contractor.

“(3) A process for independent validation by a third party of contractor maintenance.

“(d) Penalties for Noncompliance.—The Administrator shall require maintenance contracts for security-related technology deployed to airports to include penalties for noncompliance when it is determined that either preventive or corrective maintenance has not been completed according to contractual requirements and manufacturers’ specifications.”.

(b) Inspector General Assessment.—Not later than 1 year after the date of the enactment of this Act, the Inspector General of the Department of Homeland Security shall assess implementation of the requirements under section 1621 of the Homeland Security Act of 2002 (as added by subsection (a) of this section), and provide findings and recommendations with respect to the provi—
sion of training to Administration personnel, equipment
maintenance technicians, and other personnel under such
section 1621 and the availability and utilization of equip-
ment maintenance technicians employed by the Adminis-
tration.

(c) CLERICAL AMENDMENT.—The table of contents
of the Homeland Security Act of 2002 is amended by in-
serting after the item relating to section 1616 the fol-
lowing:

“Subtitle C—Maintenance of Security-Related Technology

“Sec. 1621. Maintenance validation and oversight.”.

SEC. 3219. VETTING OF AVIATION WORKERS.

(a) IN GENERAL.—Subtitle A of title XVI of the
is amended by adding after section 1601 the following new
section:

“SEC. 1602. VETTING OF AVIATION WORKERS.

“(a) IN GENERAL.—By not later than December 31,
2015, the Administrator, in coordination with the Assist-
ant Secretary for Policy of the Department, shall request
from the Director of National Intelligence access to addi-
tional data from the Terrorist Identities Datamart Envi-
rónment (TIDE) data and any or other terrorism-related
information to improve the effectiveness of the Adminis-
tration’s credential vetting program for individuals with
unescorted access to sensitive areas of airports.
“(b) Security Inspection.—By not later than December 31, 2015, the Administrator shall issue guidance for Transportation Security Inspectors to annually review airport badging office procedures for applicants seeking access to sensitive areas of airports. Such guidance shall include a comprehensive review of applicants’ Criminal History Records Check (CHRC) and work authorization documentation during the course of an inspection.

“(c) Information Sharing.—By not later than December 31, 2015, the Administrator may conduct a pilot program of the Rap Back Service, in coordination with the Director of the Federal Bureau of Investigation, to determine the feasibility of full implementation of a service through which the Administrator would be notified of a change in status of an individual holding a valid credential granting unescorted access to sensitive areas of airports across eligible Administration-regulated populations.

“(d) Procedures.—The pilot program under subsection (c) shall evaluate whether information can be narrowly tailored to ensure that the Administrator only receives notification of a change with respect to a disqualifying offense under the credential vetting program under subsection (a), as specified in 49 CFR 1542.209, and in a manner that complies with current regulations for fingerprint-based criminal history records checks. The pilot
program shall be carried out in a manner so as to ensure that, in the event that notification is made through the Rap Back Service of a change but a determination of arrest status or conviction is in question, the matter will be handled in a manner that is consistent with current regulations. The pilot program shall also be carried out in a manner that is consistent with current regulations governing an investigation of arrest status, correction of Federal Bureau of Investigation records and notification of disqualification, and corrective action by the individual who is the subject of an inquiry.

“(e) DETERMINATION AND SUBMISSION.—If the Administrator determines that full implementation of the Rap Back Service is feasible and can be carried out in a manner that is consistent with current regulations for fingerprint-based criminal history checks, including the rights of individuals seeking credentials, the Administrator shall submit such determination, in writing, to the Committee on Homeland Security of the House of Representatives and the Committee on Homeland Security and Governmental Affairs and the Committee on Commerce, Science, and Transportation of the Senate, together with information on the costs associated with such implementation, including the costs incurred by the private sector. In preparing this determination, the Administrator shall

•HR 6381 IH
consult with the Chief Civil Rights and Civil Liberties Officer of the Department to ensure that protocols are in place to align the period of retention of personally identifiable information and biometric information, including fingerprints, in the Rap Back Service with the period in which the individual who is the subject of an inquiry has a valid credential.

“(f) CREDENTIAL SECURITY.—By not later than September 30, 2015, the Administrator shall issue guidance to airports mandating that all federalized airport badging authorities place an expiration date on airport credentials commensurate with the period of time during which an individual is lawfully authorized to work in the United States.

“(g) AVIATION WORKER LAWFUL STATUS.—By not later than December 31, 2015, the Administrator shall review the denial of credentials due to issues associated with determining an applicant’s lawful status in order to identify airports with specific weaknesses and shall coordinate with such airports to mutually address such weaknesses, as appropriate.

“(h) REPORTS TO CONGRESS.—Upon completion of the determinations and reviews required under this section, the Administrator shall brief the Committee on Homeland Security and the Committee on Transportation
and Infrastructure of the House of Representatives and
the Committee on Homeland Security and Governmental
Affairs and the Committee on Commerce, Science, and
Transportation of the Senate on the results of such deter-
minations and reviews.”.

(b) CLERICAL AMENDMENT.—The table of contents
of the Homeland Security Act of 2002 is amended by in-
serting after the item relating to section 1601 the fol-
lowing new item:

“Sec. 1602. Vetting of aviation workers.”.

(c) STATUS UPDATE ON RAP BACK SERVICE PILOT
PROGRAM.—Not later than 60 days after the date of the
enactment of this Act, the Administrator of the Transpor-
tation Security Administration shall submit to the Com-
mittee on Homeland Security of the House of Representa-
tives and the Committee on Homeland Security and Gov-
ernmental Affairs and the Committee on Commerce,
Science, and Transportation of the Senate a report on the
status of plans to conduct a pilot program in coordination
with the Federal Bureau of Investigation of the Rap Back
Service in accordance with subsection (c) of section 1602
of the Homeland Security Act of 2002, as added by sub-
section (a) of this section. The report shall include details
on the business, technical, and resource requirements for
the Transportation Security Administration and pilot pro-
gram participants, and provide a timeline and goals for
the pilot program.

SEC. 3220. AVIATION SECURITY ADVISORY COMMITTEE
CONSULTATION.

(a) IN GENERAL.—The Administrator shall consult,
to the extent practicable, with the Aviation Security Advi-
sory Committee (established pursuant to section 44946 of
title 49 of the United States Code) regarding any modi-
fication to the prohibited item list prior to issuing a deter-
mination about any such modification.

(b) REPORT ON THE TRANSPORTATION SECURITY
OVERSIGHT BOARD.—Not later than 120 days after the
date of the enactment of this Act, the Secretary of Home-
land Security shall submit to the Transportation Security
Oversight Board (established pursuant to section 115 of
title 49, United States Code), the Committee on Home-
land Security of the House of Representatives, and the
Committee on Homeland Security and Governmental Af-
fairs and the Committee on Commerce, Science, and
Transportation of the Senate a report that includes gen-
eral information on how often the Board has met, the cur-
rent composition of the Board, and what activities the
Board has undertaken, consistent with the duties specified
in subsection (c) of such section. The Secretary may in-
clude in such report recommendations for changes to such
section in consideration of the provisions of section 44946
of title 49, United States Code.

(c) Technical Correction.—Subparagraph (A) of
section 44946(c)(2) of title 49, United States Code, is
amended to read as follows:

“(A) Terms.—The term of each member
of the Advisory Committee shall be 2 years but
may continue until such time as a successor
member begins serving on the Advisory Com-
mittee. A member of the Advisory Committee
may be reappointed.”.

(d) Definition.—In this section, the term “prohib-
ited item list” means the list of items passengers are pro-
hibited from carrying as accessible property or on their
persons through passenger screening checkpoints at air-
ports, into sterile areas at airports, and on board pas-
senger aircraft, pursuant to section 1540.111 of title 49,
Code of Federal Regulations (as in effect on January 1,
2015).

SEC. 3221. PRIVATE CONTRACTOR CANINE EVALUATION
AND INTEGRATION PILOT PROGRAM.

(a) In General.—Not later than 180 days after the
date of the enactment of this Act, the Administrator shall
establish a pilot program to evaluate the use, effectiveness,
and integration of privately operated explosives detection
canine teams using both the passenger screening canine
and traditional explosives detection canine methods.

(b) ELEMENTS.—The pilot program under subsection
(a) shall include the following elements:

(1) A full-time presence in three Category X,
two Category I, and one Category II airports.

(2) A duration of at least 12 months from the
time private contractor teams are operating at full
capacity.

(3) A methodology for evaluating how to integ-
strate private contractor teams into the checkpoint
area to detect explosive devices missed by mechan-
ical or human error at other points in the screening
process.

(4) Covert testing with inert improvised explo-
sive devices and accurately recreated explosives odor
traces to determine the relative effectiveness of a
full-time canine team in strengthening checkpoint
security.

(c) QUARTERLY UPDATES.—The Administrator shall
submit to the Committee on Homeland Security of the
House of Representatives and the Committee on Home-
land Security and Governmental Affairs of the Senate
written updates on the procurement, deployment, and
evaluation process related to the implementation of the
pilot program under subsection (a) for every calendar quarter after the date of the enactment of this Act.

(d) Final Report.—Not later than 90 days after the completion of the pilot program under subsection (a), the Administrator shall submit to the Committee on Homeland Security of the House of Representatives and the Committee on Homeland Security and Governmental Affairs of the Senate a final report on such pilot program.

(e) Funding.—Out of funds made available to the Office of the Secretary of Homeland Security, $6,000,000 is authorized to be used to carry out this section.

SEC. 3222. COVERT TESTING AT AIRPORTS.

(a) In General.—Not later than 1 year after the date of the enactment of this Act and annually thereafter through 2020, the Administrator shall conduct covert testing on an ongoing basis to test vulnerabilities and identify weaknesses in the measures used to secure the aviation system of the United States. The Administrator shall, on a quarterly basis if practicable, provide to the Inspector General of the Department such testing results, methodology, and data.

(b) Elements.—In carrying out the covert testing required under subsection (a), the Administrator shall—

(1) consider security screening and procedures conducted by TSA;
(2) use available threat information and intelligence to determine the types and sizes of simulated threat items and threat item-body location configurations for such covert testing;

(3) use a risk-based approach to determine the location and number of such covert testing;

(4) conduct such covert testing without notifying personnel at airports prior to such covert testing; and

(5) identify reasons for failure when TSA personnel or the screening equipment used do not identify and resolve any threat item used during such a covert test.

(e) INDEPENDENT REVIEW.—The Inspector General of the Department shall conduct covert testing of the aviation system of the United States in addition to the covert testing conducted by the Administrator under subsection (a), as appropriate, and analyze TSA covert testing results, methodology, and data provided pursuant to such subsection to determine the sufficiency of TSA covert testing protocols. The Inspector General shall, as appropriate, compare testing results of any additional covert testing conducted pursuant to this subsection with the results of TSA covert testing under subsection (a) to determine sys-
temic weaknesses in the security of the aviation system of the United States.

(d) CORRECTIVE ACTION.—Not later than 30 days upon completion of any covert testing under subsection (a), the Administrator shall make recommendations and implement corrective actions to mitigate vulnerabilities identified by such covert testing and shall notify the Inspector General of the Department of such recommendations and actions. The Inspector General shall review the extent to which such recommendations and actions are implemented and the degree to which such recommendations and actions improve the security of the aviation system of the United States.

(e) CONGRESSIONAL NOTIFICATION.—

(1) BY THE ADMINISTRATOR.—Not later than 30 days upon completion of any covert testing under subsection (a), the Administrator shall brief the Committee on Homeland Security of the House of Representatives and the Committee on Homeland Security and Governmental Affairs and the Committee on Commerce, Science, and Transportation of the Senate on the results of such covert testing.

(2) BY THE INSPECTOR GENERAL OF THE DEPARTMENT.—The Inspector General shall brief the Committee on Homeland Security of the House of
Representatives and the Committee on Homeland Security and Governmental Affairs and the Committee on Commerce, Science, and Transportation of the Senate annually on the requirements specified in this section.

(f) Rule of Construction.—Nothing in this section may be construed to prohibit the Administrator or the Inspector General of the Department from conducting covert testing of the aviation system of the United States with greater frequency than required under this section.

SEC. 3223. TRAINING FOR TRANSPORTATION SECURITY OFFICERS.

The Administrator shall, on a periodic basis, brief the Committee on Homeland Security of the House of Representatives and the Committee on Homeland Security and Governmental Affairs and the Committee on Commerce, Science, and Transportation of the Senate on the status of efforts to enhance initial and recurrent training of Transportation Security Officers.

Subtitle B—Surface Transportation Security and Other Matters

SEC. 3231. SURFACE TRANSPORTATION INSPECTORS.

(a) In General.—Section 1304(d) of the Implementing Recommendations of the 9/11 Commission Act of 2007 (6 U.S.C. 1113; Public Law 110–53) is amended—
(1) by inserting “surface” after “relevant”; and

(2) by striking “, as determined appropriate”.

(b) Report to Congress.—Not later than 1 year after the date of the enactment of this Act, the Comptroller General of the United States shall submit to the Committee on Homeland Security of the House of Representatives and the Committee on Homeland Security and Governmental Affairs and the Committee on Commerce, Science, and Transportation of the Senate a report on the efficiency and effectiveness of the Administration’s Surface Transportation Security Inspectors Program under subsection (d) of section 1304 of the Implementing Recommendations of the 9/11 Commission Act of 2007 (6 U.S.C. 1113; Public Law 110–53).

(c) Contents.—The report required under subsection (b) shall include a review of the following:

(1) The roles and responsibilities of surface transportation security inspectors.

(2) The extent to which the TSA has used a risk-based, strategic approach to determine the appropriate number of surface transportation security inspectors and resource allocation across field offices.

(3) Whether TSA’s surface transportation regulations are risk-based and whether surface transpor-
tation security inspectors have adequate experience and training to perform their day-to-day responsibilities.

(4) Feedback from regulated surface transportation industry stakeholders on the benefit of surface transportation security inspectors to the overall security of the surface transportation systems of such stakeholders and the consistency of regulatory enforcement.

(5) Whether surface transportation security inspectors have appropriate qualifications to help secure and inspect surface transportation systems.

(6) Whether TSA measures the effectiveness of surface transportation security inspectors.

(7) Any overlap between the TSA and the Department of Transportation as such relates to surface transportation security inspectors in accordance with section 1310 of the Implementing Recommendations of the 9/11 Commission Act of 2007 (6 U.S.C. 1117; Public Law 110–53).

(8) The extent to which surface transportation security inspectors review and enhance information security practices and enforce applicable information security regulations and directives.
(9) Any recommendations relating to the efficiency and effectiveness of the TSA’s surface transportation security inspectors program.

SEC. 3232. INSPECTOR GENERAL AUDIT; TSA OFFICE OF INSPECTION WORKFORCE CERTIFICATION.

(a) Inspector General Audit.—

(1) In general.—Not later than 60 days after the date of the enactment of this Act, the Inspector General of the Department shall analyze the data and methods that the Administrator uses to identify Office of Inspection employees of the Administration who meet the requirements of sections 8331(20), 8401(17), and 5545a of title 5, United States Code, and provide the relevant findings to the Administrator, including a finding on whether such data and methods are adequate and valid.

(2) Prohibition on hiring.—If the Inspector General of the Department finds that the data and methods referred to in paragraph (1) are inadequate or invalid, the Administrator may not hire any new employee to work in the Office of Inspection of the Administration until—

(A) the Administrator makes a certification described in subsection (b)(1) to the Committee on Homeland Security of the House
of Representatives and the Committee on Homeland Security and Governmental Affairs and the Committee on Commerce, Science, and Transportation of the Senate; and

(B) the Inspector General submits to such Committees a finding, not later than 30 days after the Administrator makes such certification, that the Administrator utilized adequate and valid data and methods to make such certification.

(b) TSA Office of Inspection Workforce Certification.—

(1) IN GENERAL.—The Administrator shall, by not later than 90 days after the date the Inspector General of the Department provides its findings to the Assistant Secretary under subsection (a)(1), document and certify in writing to the Committee on Homeland Security of the House of Representatives and the Committee on Homeland Security and Governmental Affairs and the Committee on Commerce, Science, and Transportation of the Senate that only those Office of Inspection employees of the Administration who meet the requirements of sections 8331(20), 8401(17), and 5545a of title 5, United States Code, are classified as criminal investigators
and are receiving premium pay and other benefits associated with such classification.

(2) **Employee Reclassification.**—The Administrator shall reclassify criminal investigator positions in the Office of Inspection of the Administration as noncriminal investigator positions or non-law enforcement positions if the individuals in such positions do not, or are not expected to, spend an average of at least 50 percent of their time performing criminal investigative duties.

(3) **Projected Cost Savings.**—

(A) **In General.**—The Administrator shall estimate the total long-term cost savings to the Federal Government resulting from the implementation of paragraph (2), and provide such estimate to the Committee on Homeland Security of the House of Representatives and the Committee on Homeland Security and Governmental Affairs and the Committee on Commerce, Science, and Transportation of the Senate by not later than 180 days after the date of enactment of this Act.

(B) **Contents.**—The estimate described in subparagraph (A) shall identify savings associated with the positions reclassified under
paragraph (2) and include, among other factors the Administrator considers appropriate, savings from—

(i) law enforcement training;

(ii) early retirement benefits;

(iii) law enforcement availability and other premium pay; and

(iv) weapons, vehicles, and communications devices.

(c) STUDY.—Not later than 180 days after the date that the Administrator submits the certification under subsection (b)(1), the Inspector General of the Department shall submit to the Committee on Homeland Security of the House of Representatives and the Committee on Homeland Security and Governmental Affairs and the Committee on Commerce, Science, and Transportation of the Senate a study—

(1) reviewing the employee requirements, responsibilities, and benefits of criminal investigators in the Office of Inspection of the Administration with criminal investigators employed at agencies adhering to the Office of Personnel Management employee classification system; and
(2) identifying any inconsistencies and costs implications for differences between the varying employee requirements, responsibilities, and benefits.

SEC. 3233. REPEAL OF BIENNIAL REPORTING REQUIREMENT FOR THE GOVERNMENT ACCOUNTABILITY OFFICE RELATING TO THE TRANSPORTATION SECURITY INFORMATION SHARING PLAN.

Subsection (u) of section 114 of title 49, United States Code, is amended by—

(1) striking paragraph (7); and

(2) redesignating paragraphs (8) and (9) as paragraphs (7) and (8), respectively.

SEC. 3234. SECURITY TRAINING FOR FRONTLINE TRANSPORTATION WORKERS.

Not later than 90 days after the date of the enactment of the Act, the Administrator shall submit to the Committee on Homeland Security of the House of Representatives and the Committee on Homeland Security and Governmental Affairs and the Committee on Commerce, Science, and Transportation of the Senate a report regarding the status of the implementation of sections 1408 (6 U.S.C. 1137) and 1534 (6 U.S.C. 1184) of the Implementing Recommendations of the 9/11 Commission Act of 2007 (Public Law 110–53). The Administrator
shall include in such report specific information on the challenges that the Administrator has encountered since the date of the enactment of the Implementing Recommendations of the 9/11 Commission Act of 2007 with respect to establishing regulations requiring the provision of basic security training to public transportation frontline employees and over-the-road bus frontline employees for preparedness for potential security threats and conditions.

SEC. 3235. FEASIBILITY ASSESSMENT.

Not later than 120 days after the date of the enactment of this Act, the Administrator shall submit to the Committee on Homeland Security of the House of Representatives and the Committee on Homeland Security and Governmental Affairs and the Committee on Commerce, Science, and Transportation of the Senate a feasibility assessment of partnering with an independent, not-for-profit organization to help provide venture capital to businesses, particularly small businesses, for commercialization of innovative homeland security technologies that are expected to be ready for commercialization in the near term and within 36 months. In conducting such feasibility assessment, the Administrator shall consider the following:

(1) Establishing an independent, not-for-profit organization, modeled after the In-Q-tel program, a
venture capital partnership between the private sector and the intelligence community (as such term is defined in section 3(4) of the National Security Act of 1947 (50 U.S.C. 3003(4)), to help businesses, particularly small businesses, commercialize innovative security-related technologies.

(2) Enhanced engagement, either through the Science and Technology Directorate of the Department of Homeland Security or directly, with the In-Q-tel program described in paragraph (1).

TITLE XXXIII—DHS SCIENCE AND TECHNOLOGY REFORM AND IMPROVEMENT

SEC. 3301. SCIENCE AND TECHNOLOGY IN SUPPORT OF HOMELAND SECURITY.

(a) In General.—Title III of the Homeland Security Act of 2002 is amended—

(1) in section 301 (6 U.S.C. 181)—

(A) by striking “There” and inserting the following new subsection:

“(a) In General.—There”; and

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

“(b) Mission.—The Directorate of Science and Technology shall be the primary research, development,
testing, and evaluation arm of the Department, responsible for coordinating the research, development, testing, and evaluation of the Department to strengthen the security and resiliency of the United States. The Directorate shall—

“(1) develop and deliver knowledge, analyses, and innovative solutions that are responsive to homeland security capability gaps and threats to the homeland identified by components and offices of the Department, the first responder community, and the Homeland Security Enterprise (as such term is defined in section 322) and that can be integrated into operations of the Department;

“(2) seek innovative, system-based solutions to complex homeland security problems and threats; and

“(3) build partnerships and leverage technology solutions developed by other Federal agencies and laboratories, State, local, and tribal governments, universities, and the private sector.”;

(2) in section 302 (6 U.S.C. 182)—

(A) in the matter preceding paragraph (1), by striking “The Secretary, acting through the Under Secretary for Science and Technology,
shall” and inserting the following new subsection:

“(a) In general.—The Secretary, acting through the Under Secretary for Science and Technology, shall carry out the mission described in subsection (b) of section 301 and shall’’;

(B) in subsection (a), as so amended by subparagraph (A) of this paragraph—

(i) in paragraph (1), by inserting “and serving as the senior scientific advisor to the Secretary” before the semicolon at the end;

(ii) in paragraph (2)—

(I) by striking “national”;

(II) by striking “biological,” and inserting “biological,”; and

(III) by inserting “that may serve as a basis of a national strategy” after “terrorist threats”;

(iii) in paragraph (3)—

(I) by striking “the Under Secretary for Intelligence and Analysis and the Assistant Secretary for Infrastructure Protection” and inserting
“components and offices of the Department”; and

(II) by inserting “terrorist” before “threats”;

(iv) in paragraph (4), by striking “except that such responsibility does not extend to human health-related research and development activities” and inserting the following: “including coordinating with relevant components and offices of the Department appropriate to—

“(A) identify and prioritize technical capability requirements and create solutions that include researchers, the private sector, and operational end users; and

“(B) develop capabilities to address issues on research, development, testing, evaluation, technology, and standards for the first responder community,

except that such responsibility does not extend to the human health-related research and development activities;”;

(v) in paragraph (5)(A), by striking “biological,” and inserting “biological,”;
(vi) by amending paragraph (12) to read as follows:

“(12) coordinating and integrating all research, development, demonstration, testing, and evaluation activities of the Department, including through a centralized Federal clearinghouse established pursuant to paragraph (1) of section 313(b) for information relating to technologies that would further the mission of the Department, and providing advice, as necessary, regarding major acquisition programs;”;

(vii) in paragraph (13), by striking “and” at the end;

(viii) in paragraph (14), by striking the period at the end and inserting a semicolon; and

(ix) by adding at the end the following new paragraphs:

“(15) establishing a process that—

“(A) includes consideration by Directorate leadership, senior component leadership, first responders, and outside expertise;

“(B) is strategic, transparent, and repeatable with a goal of continuous improvement;
“(C) through which research and development projects undertaken by the Directorate are assessed on a regular basis; and

“(D) includes consideration of metrics to ensure research and development projects meet Directorate and Department goals and inform departmental budget and program planning;

“(16) developing and overseeing the administration of guidelines for periodic external review of departmental research and development programs or activities, including through—

“(A) consultation with experts, including scientists and practitioners, regarding the research and development activities conducted by the Directorate of Science and Technology; and

“(B) biennial independent, external review—

“(i) initially at the division level; or

“(ii) when divisions conduct multiple programs focused on significantly different subjects, at the program level;

“(17) partnering with components and offices of the Department to develop and deliver knowledge, analyses, and innovative solutions that are responsive to identified homeland security capability gaps
and threats to the homeland and raise the science-based, analytic capability and capacity of appropriate individuals throughout the Department by providing guidance on how to better identify homeland security capability gaps and threats to the homeland that may be addressed through a technological solution and by partnering with such components and offices to—

“(A) support technological assessments of major acquisition programs throughout the acquisition lifecycle;

“(B) help define appropriate technological requirements and perform feasibility analysis;

“(C) assist in evaluating new and emerging technologies against homeland security capability gaps and terrorist threats;

“(D) support evaluation of alternatives;

“(E) improve the use of technology Department-wide; and

“(F) provide technical assistance in the development of acquisition lifecycle cost for technologies;

“(18) acting as a coordinating office for technology development for the Department by helping components and offices define technological require-
ments, and building partnerships with appropriate
tentities (such as within the Department and with
other Federal agencies and laboratories, State, local,
and tribal governments, universities, and the private
sector) to help each such component and office at-
tain the technology solutions it needs; and

“(19) coordinating with organizations that pro-
vide venture capital to businesses, particularly small
businesses, as appropriate, to assist in the commer-
cialization of innovative homeland security tech-
nologies that are expected to be ready for commer-
cialization in the near term and within 36 months.”;
and

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

“(b) REVIEW OF RESPONSIBILITIES.—Not later than
180 days after the date of the enactment of this sub-
section, the Under Secretary for Science and Technology
shall submit to the Committee on Homeland Security and
the Committee on Science, Space, and Technology of the
House of Representatives and the Committee on Home-
land Security and Governmental Affairs of the Senate a
report on the implementation of paragraphs (2) (including
how the policy and strategic plan under such paragraph
may serve as a basis for a national strategy referred to
in such paragraph), (11), (12), (13), (16), and (17) of subsection (a).”;

(3) in section 303(1) (6 U.S.C. 183(1)), by striking subparagraph (F);

(4) in section 305 (6 U.S.C. 185)—

(A) by striking “The” and inserting the following new subsection:

“(a) ESTABLISHMENT.—The”; and

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

“(b) CONFLICTS OF INTEREST.—The Secretary shall review and revise, as appropriate, the policies of the Department relating to personnel conflicts of interest to ensure that such policies specifically address employees of federally funded research and development centers established pursuant to subsection (a) who are in a position to make or materially influence research findings or agency decisionmaking.”;

(5) in section 306 (6 U.S.C. 186)—

(A) in subsection (c), by adding at the end the following new sentence: “If such regulations are issued, the Under Secretary shall report to the Committee on Homeland Security and the Committee on Science, Space, and Technology of the House of Representatives and the Com-
mittee on Homeland Security and Governmental Affairs of the Senate prior to such issuance.”; and (B) by amending subsection (d) to read as follows:

“(d) PERSONNEL.—In hiring personnel for the Directorate of Science and Technology, the Secretary shall have the hiring and management authorities described in section 1101 of the Strom Thurmond National Defense Authorization Act for Fiscal Year 1999 (5 U.S.C. 3104 note; Public Law 105–261). The term of appointments for employees under subsection (c)(1) of such section may not exceed 5 years before the granting of any extension under subsection (c)(2) of such section.”;

(6) in section 308 (6 U.S.C. 188)— (A) in subsection (b)(2)— (i) in subparagraph (B)— (I) in clause (iv), by striking “and nuclear countermeasures or detection” and inserting “nuclear, and explosives countermeasures or detection (which may include research into remote sensing and remote imaging)”; and
(II) by adding after clause (xiv) the following new clause:

“(xv) Cybersecurity.”; and

(ii) by amending subparagraph (D) to read as follows:

“(D) **Annual report to Congress.**—Not later than 1 year after the date of the enactment of this subparagraph and annually thereafter, the Secretary shall submit to Congress a report on the implementation of this section. Each such report shall—

“(i) indicate which center or centers have been designated pursuant to this section;

“(ii) describe how such designation or designations enhance homeland security;

“(iii) provide information on any decisions to revoke or modify such designation or designations;

“(iv) describe research that has been tasked and completed by each center that has been designated during the preceding year;
“(v) describe funding provided by the Secretary for each center under clause (iv) for that year; and

“(vi) describe plans for utilization of each center or centers in the forthcoming year.”; and

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

“(d) Test, Evaluation, and Standards Division.—

“(1) Establishment.—There is established in the Directorate of Science and Technology a Test, Evaluation, and Standards Division.

“(2) Director.—The Test, Evaluation, and Standards Division shall be headed by a Director of Test, Evaluation, and Standards, who shall be appointed by the Secretary and report to the Under Secretary for Science and Technology.

“(3) Responsibilities, Authorities, and Functions.—The Director of Test, Evaluation, and Standards—

“(A) through the Under Secretary for Science and Technology, serve as an adviser to the Secretary and the Under Secretary of Man-
agement on all test and evaluation or standards activities in the Department; and

“(B) shall—

“(i) establish and update as necessary test and evaluation policies for the Department, including policies to ensure that operational testing is done at facilities that already have relevant and appropriate safety and material certifications to the extent such facilities are available;

“(ii) oversee and ensure that adequate test and evaluation activities are planned and conducted by or on behalf of components and offices of the Department with respect to major acquisition programs of the Department, as designated by the Secretary, based on risk, acquisition level, novelty, complexity, and size of any such acquisition program, or as otherwise established in statute;

“(iii) review major acquisition program test reports and test data to assess the adequacy of test and evaluation activities conducted by or on behalf of components and offices of the Department, in-
cluding test and evaluation activities
planned or conducted pursuant to clause
(ii); and

“(iv) review available test and evaluation infrastructure to determine whether
the Department has adequate resources to
carry out its testing and evaluation respons-
sibilities, as established under this title.

“(4) LIMITATION.—The Test, Evaluation, and
Standards Division is not required to carry out oper-
ational testing of major acquisition programs.

“(5) EVALUATION OF DEPARTMENT OF DE-
FENSE TECHNOLOGIES.—The Director of Test,
Evaluation, and Standards may evaluate tech-
nologies currently in use or being developed by the
Department of Defense to assess whether such tech-
nologies can be leveraged to address homeland secu-

rity capability gaps.”;

(7) in section 309(a) (6 U.S.C. 189(a)), by add-
ing at the end the following new paragraph:

“(3) TREATMENT OF CERTAIN FUNDS.—Not-
withstanding any other provision of law, any funds
provided to a Department of Energy national labora-
tory by the Department may not be treated as an
assisted acquisition.”;
(8) in section 310 (6 U.S.C. 190), by adding at the end the following new subsection:

“(e) SUCCESSOR FACILITY.—Any successor facility to the Plum Island Animal Disease Center, including the National Bio and Agro-Defense Facility (NBAF) under construction as of the date of the enactment of this subsection, which is intended to replace the Plum Island Animal Disease Center shall be subject to the requirements of this section in the same manner and to the same extent as the Plum Island Animal Disease Center under this section.”;

(9) in section 311 (6 U.S.C. 191)—

(A) in subsection (b)—

(i) in paragraph (1)—

(I) by striking “20 members” and inserting “not fewer than 15 and not more than 30”; and

(II) by inserting “academia, national labs, private industry, and” after “representatives of”; 

(ii) by redesignating paragraph (2) as paragraph (3); and

(iii) by inserting after paragraph (1) the following new paragraph:
“(2) SUBCOMMITTEES.—The Advisory Committee may establish subcommittees that focus on research and development challenges, as appropriate.”;

(B) in subsection (c)—

(i) in paragraph (1), by inserting “on a rotating basis” before the period at the end;

(ii) by striking paragraph (2) and redesignating paragraph (3) as paragraph (2); and

(iii) in paragraph (2), as so redesignated, by striking “be appointed” and inserting “serve”;

(C) in subsection (e), in the second sentence, by striking “the call of”;

(D) in subsection (h)—

(i) in paragraph (1)—

(I) in the first sentence—

(aa) by striking “render” and inserting “submit”; and

(bb) by striking “Congress” and inserting “the appropriate congressional committees”; and
(II) in the second sentence, by inserting ‘‘, and incorporate the findings and recommendations of the Advisory Committee subcommittees,’’ before ‘‘during’’; and

(ii) in paragraph (2)—

(I) by striking ‘‘render’’ and inserting ‘‘submit’’; and

(II) by striking ‘‘Congress’’ and inserting ‘‘the Committee on Homeland Security and the Committee on Science, Space, and Technology of the House of Representatives and the Committee on Homeland Security and Governmental Affairs of the Senate’’;

(E) in subsection (i), by inserting ‘‘, except that the Advisory Committee shall file a charter with Congress every 2 years in accordance with subsection (b)(2) of such section (14)’’;

(F) in subsection (j), by striking ‘‘2008’’ and inserting ‘‘2020’’;

(10) in section 313 (6 U.S.C. 193)—

(A) by redesignating subsection (c) as subsection (d); and
(B) by inserting after subsection (b) the following new subsection:

“(c) APPLICATION OF PROGRAM.—The Secretary, acting through the Under Secretary for Science and Technology, shall use the program established under subsection (a) to—

“(1) enhance the cooperation between components and offices of the Department on projects that have similar goals, timelines, or outcomes;

“(2) ensure the coordination of technologies to eliminate unnecessary duplication of research and development;

“(3) ensure technologies are accessible for component and office use on a Department website; and

“(4) carry out any additional purpose the Secretary determines necessary.”; and

(11) by adding after section 317 (6 U.S.C. 195e) the following new sections:

“SEC. 318. IDENTIFICATION AND PRIORITIZATION OF RESEARCH AND DEVELOPMENT.

“(a) IN GENERAL.—Not later than 180 days after the date of the enactment of this section, the Under Secretary for Science and Technology shall establish a process to define, identify, prioritize, fund, and task the basic and applied homeland security research and development ac-
activities of the Directorate of Science and Technology to meet the needs of the components and offices of the Department, the first responder community, and the Homeland Security Enterprise (as such term is defined in section 322).

“(b) Process.—The process established under subsection (a) shall—

“(1) be responsive to near-, mid-, and long-term needs, including unanticipated needs to address emerging terrorist threats;

“(2) utilize gap analysis and risk assessment tools where available and applicable;

“(3) include protocols to assess—

“(A) off-the-shelf technology to determine if an identified homeland security capability gap or threat to the homeland can be addressed through the acquisition process instead of commencing research and development of technology to address such capability gap or threat; and

“(B) communication and collaboration for research and development activities pursued by other executive agencies, to determine if technology can be leveraged to identify and address homeland security capability gaps or threats to
the homeland and avoid unnecessary duplication of efforts;

“(4) provide for documented and validated research and development requirements;

“(5) strengthen first responder participation to identify and prioritize homeland security technological gaps, including by—

“(A) soliciting feedback from appropriate national associations and advisory groups representing the first responder community and first responders within the components and offices of the Department; and

“(B) establishing and promoting a publicly accessible portal to allow the first responder community to help the Directorate of Science and Technology develop homeland security research and development goals;

“(6) institute a mechanism to publicize the Department’s homeland security technology priorities for the purpose of informing Federal, State, and local governments, first responders, and the private sector;

“(7) establish considerations to be used by the Directorate in selecting appropriate research entities, including the national laboratories, federally
funded research and development centers, university-based centers, and the private sector, to carry out research and development requirements;

“(8) incorporate feedback derived as a result of the mechanism established in section 323, ensuring the Directorate is utilizing regular communication with components and offices of the Department; and

“(9) include any other criteria or measures the Under Secretary for Science and Technology considers necessary for the identification and prioritization of research requirements.

“SEC. 319. DEVELOPMENT OF DIRECTORATE STRATEGY AND RESEARCH AND DEVELOPMENT PLAN.

“(a) Strategy.—

“(1) In general.—Not later than 1 year after the date of the enactment of this section, the Under Secretary for Science and Technology shall develop and submit to the Committee on Homeland Security and the Committee on Science, Space, and Technology of the House of Representatives and the Committee on Homeland Security and Governmental Affairs of the Senate a strategy to guide the activities of the Directorate of Science and Technology. Such strategy shall be updated at least once every 5 years and shall identify priorities and objectives
for the development of science and technology solutions and capabilities addressing homeland security operational needs. Such strategy shall include the coordination of such priorities and activities within the Department. Such strategy shall take into account the priorities and needs of stakeholders in the Homeland Security Enterprise (as such term is defined in section 322). In developing such strategy, efforts shall be made to support collaboration and avoid unnecessary duplication across the Federal Government. Such strategy shall be risk-based and aligned with other strategic guidance provided by—

“(A) the National Strategy for Homeland Security;

“(B) the Quadrennial Homeland Security Review; and

“(C) any other relevant strategic planning documents, as determined by the Under Secretary.

“(2) CONTENTS.—The strategy required under paragraph (1) shall be prepared in accordance with applicable Federal requirements and guidelines, and shall include the following:

“(A) An identification of the long-term strategic goals, objectives, and metrics of the
Directorate, including those to address terrorist threats.

“(B) A technology transition strategy for the programs of the Directorate.

“(C) Short- and long-term strategic goals, and objectives for increasing the number of designations and certificates issued under subtitle G of title VIII, including cybersecurity technologies that could significantly reduce, or mitigate the effects of, cybersecurity risks (as such term is defined in subsection (a)(1) of the second section 226, relating to the national cybersecurity and communications integration center), without compromising the quality of the evaluation of applications for such designations and certificates.

“(b) FIVE-YEAR RESEARCH AND DEVELOPMENT PLAN.—

“(1) IN GENERAL.—The Under Secretary for Science and Technology shall develop, and update at least once every 5 years, a 5-year research and development plan for the activities of the Directorate of Science and Technology. The Under Secretary shall develop the first such plan by the date that is
not later than 1 year after the date of the enactment of this section.

“(2) CONTENTS.—Each 5-year research and development plan developed and revised under subsection (a) shall—

“(A) define the Directorate of Science and Technology’s research, development, testing, and evaluation activities, priorities, performance metrics, and key milestones and deliverables for, as the case may be, the 5-fiscal-year period from 2016 through 2020, and for each 5-fiscal-year period thereafter;

“(B) describe, for the activities of the strategy developed under subsection (a), the planned annual funding levels for the period covered by each such 5-year research and development plan;

“(C) indicate joint investments with other Federal partners where applicable, and enhanced coordination, as appropriate, with organizations as specified in paragraph (19) of section 302;

“(D) analyze how the research programs of the Directorate support achievement of the
strategic goals and objectives identified in the strategy required under subsection (a);

“(E) describe how the activities and programs of the Directorate meet the requirements or homeland security capability gaps or threats to the homeland identified by customers within and outside of the Department, including the first responder community; and

“(F) describe the policies of the Directorate regarding the management, organization, and personnel of the Directorate.

“(3) SCOPE.—The Under Secretary for Science and Technology shall ensure that each 5-year research and development plan developed and revised under subsection (a)—

“(A) reflects input from a wide range of stakeholders; and

“(B) takes into account how research and development by other Federal, State, private sector, and nonprofit institutions contributes to the achievement of the priorities identified in each plan, and avoids unnecessary duplication with such efforts.

“(4) REPORTS.—The Under Secretary for Science and Technology shall submit to the Com-
mittee on Homeland Security and the Committee on
Science, Space, and Technology of the House of
Representatives and the Committee on Homeland
Security and Governmental Affairs of the Senate an
annual report for 7 years beginning not later than
1 year after the date of the development of the ini-
tial 5-year research and development plan under
paragraph (1) on the status and results to date of
the implementation of such plan and the updates to
such plan, including—

“(A) a summary of the research and devel-
opment activities for the previous fiscal year in
each mission area, including such activities to
address homeland security risks, including
threats, vulnerabilities, and consequences, and a
summary of the coordination activities under-
taken by the Directorate of Science and Tech-
ology for components and offices of the De-
partment, together with the results of the proc-
ess specified in paragraph (15) of section 302;

“(B) clear links between the Directorate’s
budget and each mission area or program, in-
cluding those mission areas or programs to ad-
dress homeland security risks, including
threats, vulnerabilities, and consequences, speci-
fying which mission areas or programs fall
under which budget lines, and clear links be-
tween Directorate coordination work and prior-
ities and annual expenditures for such work and
priorities, including joint investments with other
Federal partners, where applicable;

“(C) an assessment of progress of the re-
search and development activities based on the
performance metrics and milestones set forth in
such plan; and

“(D) any changes to such plan.

“SEC. 320. MONITORING OF PROGRESS.

“(a) IN GENERAL.—The Under Secretary for Science
and Technology shall establish and utilize a system to
track the progress of the research, development, testing,
and evaluation activities undertaken by the Directorate of
Science and Technology, and shall provide to the Com-
mittee on Homeland Security and the Committee on
Science, Space, and Technology of the House of Rep-
resentatives and the Committee on Homeland Security
and Governmental Affairs of the Senate and customers of
such activities, at a minimum on a biannual basis, regular
updates on such progress.

“(b) REQUIREMENTS.—In order to provide the
progress updates required under subsection (a), the Under
Secretary for Science and Technology shall develop a system that—

“(1) monitors progress toward project milestones identified by the Under Secretary;

“(2) maps progress toward deliverables identified in each 5-year research and development plan required under section 319(b);

“(3) generates up-to-date reports to customers that transparently disclose the status and progress of research, development, testing, and evaluation efforts of the Directorate of Science and Technology; and

“(4) allows the Under Secretary to report the number of products and services developed by the Directorate that have been transitioned into acquisition programs and resulted in successfully fielded technologies.

“(c) EVALUATION METHODS.—

“(1) EXTERNAL INPUT, CONSULTATION, AND REVIEW.—The Under Secretary for Science and Technology shall implement procedures to engage outside experts to assist in the evaluation of the progress of research, development, testing, and evaluation activities of the Directorate of Science and Technology, including through—
“(A) consultation with experts, including
scientists and practitioners, to gather inde-
pendent expert peer opinion and advice on a
project or on specific issues or analyses con-
ducted by the Directorate; and

“(B) periodic, independent, external review
to assess the quality and relevance of the Direc-
torate’s programs and projects.

“(2) COMPONENT FEEDBACK.—The Under Sec-
retary for Science and Technology shall establish a
formal process to collect feedback from customers of
the Directorate of Science and Technology on the
performance of the Directorate that includes—

“(A) appropriate methodologies through
which the Directorate can assess the quality
and usefulness of technology and services deliv-
ered by the Directorate;

“(B) development of metrics for measuring
the usefulness of any technology or service pro-
vided by the Directorate; and

“(C) standards for high-quality customer
service.
SEC. 321. HOMELAND SECURITY SCIENCE AND TECHNOLOGY FELLOWS PROGRAM.

(a) Establishment.—The Secretary, acting through the Under Secretary for Science and Technology and the Under Secretary for Management, shall establish a fellows program, to be known as the Homeland Security Science and Technology Fellows Program (in this section referred to as the ‘Program’), under which the Under Secretary for Science and Technology, in coordination with the Office of University Programs of the Department, shall facilitate the placement of fellows in relevant scientific or technological fields for up to 2 years in components and offices of the Department with a need for scientific and technological expertise.

(b) Utilization of Fellows.—

(1) In general.—Under the Program, the Department may employ fellows—

(A) for the use of the Directorate of Science and Technology; or

(B) for the use of a component or office of the Department outside the Directorate, under a memorandum of agreement with the head of such a component or office under which such component or office will reimburse the Directorate for the costs of such employment.
“(2) RESPONSIBILITIES.—Under an agreement referred to in subparagraph (B) of paragraph (1)—

“(A) the Under Secretary for Science and Technology and the Under Secretary for Management shall—

“(i) solicit and accept applications from individuals who are currently enrolled in or who are graduates of postgraduate programs in scientific and engineering fields related to the promotion of securing the homeland or critical infrastructure sectors;

“(ii) screen applicants and interview them as appropriate to ensure that such applicants possess the appropriate level of scientific and engineering expertise and qualifications;

“(iii) provide a list of qualified applicants to the heads of components and offices of the Department seeking to utilize qualified fellows;

“(iv) subject to the availability of appropriations, pay financial compensation to such fellows;
“(v) coordinate with the Chief Security Officer to facilitate and expedite provision of security and suitability clearances to such fellows, as appropriate; and

“(vi) otherwise administer all aspects of the employment of such fellows with the Department; and

“(B) the head of the component or office of the Department utilizing a fellow shall—

“(i) select such fellow from the list of qualified applicants provided by the Under Secretary;

“(ii) reimburse the Under Secretary for the costs of employing such fellow, including administrative costs; and

“(iii) be responsible for the day-to-day management of such fellow.

“(c) Applications From Nonprofit Organizations.—The Under Secretary for Science and Technology may accept an application under subsection (b)(2)(A) that is submitted by a nonprofit organization on behalf of individuals whom such nonprofit organization has determined may be qualified applicants under the Program.
“SEC. 322. CYBERSECURITY RESEARCH AND DEVELOPMENT.

“(a) In General.—The Under Secretary for Science and Technology shall support research, development, testing, evaluation, and transition of cybersecurity technology, including fundamental research to improve the sharing of information, analytics, and methodologies related to cybersecurity risks and incidents, consistent with current law.

“(b) Activities.—The research and development supported under subsection (a) shall serve the components of the Department and shall—

“(1) advance the development and accelerate the deployment of more secure information systems;

“(2) improve and create technologies for detecting attacks or intrusions, including real-time continuous diagnostics and real-time analytic technologies;

“(3) improve and create mitigation and recovery methodologies, including techniques and policies for real-time containment of attacks, and development of resilient networks and information systems;

“(4) support, in coordination with the private sector, the review of source code that underpins critical infrastructure information systems;

“(5) develop and support infrastructure and tools to support cybersecurity research and development efforts, including modeling, testbeds, and data
sets for assessment of new cybersecurity technologies; 

“(6) assist the development and support of technologies to reduce vulnerabilities in industrial control systems; and 

“(7) develop and support cyber forensics and attack attribution.

“(c) COORDINATION.—In carrying out this section, the Under Secretary for Science and Technology shall co-ordinate activities with—

“(1) the Under Secretary appointed pursuant to section 103(a)(1)(H); 

“(2) the heads of other relevant Federal departments and agencies, including the National Science Foundation, the Defense Advanced Research Projects Agency, the Information Assurance Directorate of the National Security Agency, the National Institute of Standards and Technology, the Department of Commerce, the Networking and Information Technology Research and Development Program Office, Sector Specific Agencies for critical infrastructure, and other appropriate working groups established by the President to identify unmet needs and cooperatively support activities, as appropriate; and 

“(3) industry and academia.
“(d) Transition to Practice.—The Under Secretary for Science and Technology shall support projects through the full life cycle of such projects, including research, development, testing, evaluation, pilots, and transitions. The Under Secretary shall identify mature technologies that address existing or imminent cybersecurity gaps in public or private information systems and networks of information systems, identify and support necessary improvements identified during pilot programs and testing and evaluation activities, and introduce new cybersecurity technologies throughout the Homeland Security Enterprise through partnerships and commercialization. The Under Secretary shall target federally funded cybersecurity research that demonstrates a high probability of successful transition to the commercial market within 2 years and that is expected to have notable impact on the cybersecurity of the information systems or networks of information systems of the United States.

“(e) Definitions.—In this section:

“(1) Cybersecurity Risk.—The term ‘cybersecurity risk’ has the meaning given such term in the second section 226, relating to the national cybersecurity and communications integration center.

“(2) Homeland Security Enterprise.—The term ‘Homeland Security Enterprise’ means relevant
governmental and nongovernmental entities involved
in homeland security, including Federal, State, local,
and tribal government officials, private sector rep-
resentatives, academics, and other policy experts.

“(3) INCIDENT.—The term ‘incident’ has the
meaning given such term in the second section 226,
relating to the national cybersecurity and commu-
ications integration center.

“(4) INFORMATION SYSTEM.—The term ‘infor-
mation system’ has the meaning given that term in
section 3502(8) of title 44, United States Code.

“SEC. 323. INTEGRATED PRODUCT TEAMS.

“(a) IN GENERAL.—The Secretary shall establish in-
tegrated product teams to serve as a central mechanism
for the Department to identify, coordinate, and align re-
search and development efforts with departmental mis-
sions. Each team shall be managed by the Under Sec-
etary for Science and Technology and the relevant senior
leadership of operational components, and shall be respon-
sible for the following:

“(1) Identifying and prioritizing homeland secu-

ity capability gaps or threats to the homeland with-
in a specific mission area and technological solutions
to address such gaps.
“(2) Identifying ongoing departmental research and development activities and component acquisitions of technologies that are outside of departmental research and development activities to address a specific mission area.

“(3) Assessing the appropriateness of a technology to address a specific mission area.

“(4) Identifying unnecessary redundancy in departmental research and development activities within a specific mission area.

“(5) Informing the Secretary and the annual budget process regarding whether certain technological solutions are able to address homeland security capability gaps or threats to the homeland within a specific mission area.

“(b) CONGRESSIONAL OVERSIGHT.—Not later than 2 years after the date of enactment of this section, the Secretary shall provide to the Committee on Homeland Security and the Committee on Science, Space, and Technology of the House of Representatives and the Committee on Homeland Security and Governmental Affairs of the Senate information on the impact and effectiveness of the mechanism described in subsection (a) on research and development efforts, component relationships, and how the process has informed the research and development budget
and enhanced decisionmaking, including acquisition decisionmaking, at the Department. The Secretary shall seek feedback from the Under Secretary for Science and Technology, Under Secretary for Management, and the senior leadership of operational components regarding the impact and effectiveness of such mechanism and include such feedback in the information provided under this subsection.

"SEC. 324. HOMELAND SECURITY-STEM SUMMER INTERNSHIP PROGRAM."

"(a) In General.—The Under Secretary for Science and Technology shall establish a Homeland Security-STEM internship program (in this section referred to as the 'program') to carry out the objectives of this subtitle.

"(b) Program.—The program shall provide students with exposure to Department mission-relevant research areas, including threats to the homeland, to encourage such students to pursue STEM careers in homeland security related fields. Internships offered under the program shall be for up to 10 weeks during the summer.

"(c) Eligibility.—The Under Secretary for Science and Technology shall develop criteria for participation in the program, including the following:

"(1) At the time of application, an intern shall—
“(A) have successfully completed not less than 1 academic year of study at an institution of higher education in a STEM field;

“(B) be enrolled in a course of study in a STEM field at an institution of higher education; and

“(C) plan to continue such course of study or pursue an additional course of study in a STEM field at an institution of higher education in the academic year following the internship.

“(2) An intern shall be pursuing career goals aligned with the Department’s mission, goals, and objectives.

“(3) Any other criteria the Under Secretary determines appropriate.

“(d) COOPERATION.—The program shall be administered in cooperation with the university-based centers for homeland security under section 308. Interns in the program shall be provided hands-on research experience and enrichment activities focused on Department research areas.

“(e) ACADEMIC REQUIREMENTS; OPERATION.—The Under Secretary for Science and Technology shall determine the academic requirements, other selection criteria,
and standards for successful completion of each internship period in the program. The Under Secretary shall be responsible for the design, implementation, and operation of the program.

“(f) **Research Mentors.**—The Under Secretary for Science and Technology shall ensure that each intern in the program is assigned a research mentor to act as counselor and advisor and provide career-focused advice.

“(g) **Outreach to Certain Under-Represented Students.**—The Under Secretary for Science and Technology shall conduct outreach to students who are members of groups under-represented in STEM careers to encourage their participation in the program.

“(h) **Institution of Higher Education Defined.**—In this section, the term ‘institution of higher education’ has the meaning given the term in section 102 of the Higher Education Act of 1965 (20 U.S.C. 1002), except that the term does not include institutions described in subparagraph (C) of such section 102(a)(1).”

(b) **Effective Date.**—The amendments made by subsection (a) shall take effect on the date that is 30 days after the date of the enactment of this section.

(e) **Clerical Amendment.**—The table of contents in section 1(b) of the Homeland Security Act of 2002 is
amended by inserting after the item relating to section 317 the following new items:

“Sec. 318. Identification and prioritization of research and development.
Sec. 319. Development of Directorate strategy and research and development plan.
Sec. 320. Monitoring of progress.
Sec. 321. Homeland Security Science and Technology Fellows Program.
Sec. 322. Cybersecurity research and development.
Sec. 323. Integrated product teams.
Sec. 324. Homeland Security-STEM summer internship program.”.

(d) RESEARCH AND DEVELOPMENT PROJECTS.—

Section 831 of the Homeland Security Act of 2002 (6 U.S.C. 391) is amended—

(1) in subsection (a)—

(A) in the matter preceding paragraph (1), by striking “2015” and inserting “2020”;

(B) in paragraph (1), by striking the last sentence; and

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

“(3) PRIOR APPROVAL.—In any case in which a component or office of the Department seeks to utilize the authority under this section, such office or component shall first receive prior approval from the Secretary by providing to the Secretary a proposal that includes the rationale for the use of such authority, the funds to be spent on the use of such authority, and the expected outcome for each project that is the subject of the use of such authority. In
such a case, the authority for evaluating the proposal may not be delegated by the Secretary to anyone other than the Under Secretary for Management.”;

(2) in subsection (e)—

(A) in paragraph (1), in the matter preceding subparagraph (A), by striking “2015” and inserting “2020”; and

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

“(2) REPORT.—The Secretary shall annually submit to the Committee on Homeland Security and the Committee on Science, Space, and Technology of the House of Representatives and the Committee on Homeland Security and Governmental Affairs of the Senate a report detailing the projects for which the authority granted by subsection (a) was used, the rationale for such use, the funds spent using such authority, the extent of cost-sharing for such projects among Federal and non-Federal sources, the extent to which use of such authority has addressed a homeland security capability gap or threat to the homeland identified by the Department, the total amount of payments, if any, that were received by the Federal Government as a result of the use of
such authority during the period covered by each
such report, the outcome of each project for which
such authority was used, and the results of any au-
dits of such projects.”; and

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

“(e) TRAINING.—The Secretary shall develop a train-
ing program for acquisitions staff in the use of other
transaction authority to help ensure the appropriate use
of such authority.

“(f) OTHER TRANSACTION AUTHORITY DEFINED.—
In this section, the term ‘other transaction authority’
means authority under subsection (a).”.

(e) AMENDMENT TO DEFINITION.—Paragraph (2) of
subsection (a) of the second section 226 of the Homeland
Security Act of 2002 (6 U.S.C. 148; relating to the na-
tional cybersecurity and communications integration cen-
ter) is amended to read as follows:

“(2) INCIDENT.—The term ‘incident’ means an
occurrence that actually or imminently jeopardizes,
without lawful authority, the integrity, confiden-
tiality, or availability of information on an informa-
tion system, or actually or imminently jeopardizes,
without lawful authority, an information system.”.

(f) GAO STUDY OF UNIVERSITY-BASED CENTERS.—
IN GENERAL.—Not later than 120 days after the date of the enactment of this Act, the Comptroller General of the United States shall initiate a study to assess the university-based centers for homeland security program authorized by section 308(b)(2) of the Homeland Security Act of 2002 (6 U.S.C. 188(b)(2)), and provide recommendations to the Committee on Homeland Security and the Committee on Science, Space, and Technology of the House of Representatives and the Committee on Homeland Security and Governmental Affairs of the Senate for appropriate improvements.

SUBJECT MATTERS.—The study required under subsection (a) shall include the following:

(A) A review of the Department of Homeland Security’s efforts to identify key areas of study needed to support the homeland security mission, and criteria that the Department utilized to determine those key areas for which the Department should maintain, establish, or eliminate university-based centers.

(B) A review of the method by which university-based centers, federally funded research and development centers, and Department of Energy national laboratories receive tasking
from the Department of Homeland Security, including a review of how university-based research is identified, prioritized, and funded.

(C) A review of selection criteria for designating university-based centers and a weighting of such criteria.

(D) An examination of best practices from other agencies’ efforts to organize and use university-based research to support their missions.

(E) A review of the Department of Homeland Security’s criteria and metrics to measure demonstrable progress achieved by university-based centers in fulfilling Department taskings, and mechanisms for delivering and disseminating the research results of designated university-based centers within the Department and to other Federal, State, and local agencies.

(F) An examination of the means by which academic institutions that are not designated or associated with the designated university-based centers can optimally contribute to the research mission of the Directorate of Science and Technology of the Department of Homeland Security.
(G) An assessment of the interrelationship between the different university-based centers and the degree to which outreach and collaboration among a diverse array of academic institutions is encouraged by the Department of Homeland Security, particularly with historically Black colleges and universities and minority-serving institutions.

(H) A review of any other essential elements of the programs determined in the conduct of the study.

(g) PRIZE AUTHORITY.—The Under Secretary for Science and Technology of the Department of Homeland Security shall utilize, as appropriate, prize authority granted pursuant to current law.

(h) PROHIBITION ON NEW FUNDING.—No funds are authorized to be appropriated to carry out this section and the amendments made by this section. Such section and amendments shall be carried out using amounts otherwise appropriated or made available for such purposes.

TITLE XXXIV—REVIEW OF UNIVERSITY-BASED CENTERS

SEC. 3401. REVIEW OF UNIVERSITY-BASED CENTERS.

(a) GAO STUDY OF UNIVERSITY-BASED CENTERS.—Not later than 120 days after the date of enactment of
this Act, the Comptroller General of the United States shall initiate a study to assess the university-based centers for homeland security program authorized by section 308(b)(2) of the Homeland Security Act of 2002 (6 U.S.C. 188(b)(2)), and provide recommendations to the Committee on Homeland Security and the Committee on Science, Space, and Technology of the House of Representatives and the Committee on Homeland Security and Governmental Affairs of the Senate for appropriate improvements.

(b) Subject Matters.—The study under subsection (a) shall include the following:

(1) A review of the Department of Homeland Security’s efforts to identify key areas of study needed to support the homeland security mission, and criteria that the Department utilized to determine those key areas for which the Department should maintain, establish, or eliminate university-based centers.

(2) A review of the method by which university-based centers, federally funded research and development centers, and Department of Energy national laboratories receive tasking from the Department of Homeland Security, including a review of how uni-
versity-based research is identified, prioritized, and funded.

(3) A review of selection criteria for designating university-based centers and a weighting of such criteria.

(4) An examination of best practices from other agencies’ efforts to organize and use university-based research to support their missions.

(5) A review of the Department of Homeland Security’s criteria and metrics to measure demonstrable progress achieved by university-based centers in fulfilling Department taskings, and mechanisms for delivering and disseminating the research results of designated university-based centers within the Department and to other Federal, State, and local agencies.

(6) An examination of the means by which academic institutions that are not designated or associated with the designated university-based centers can optimally contribute to the research mission of the Directorate of Science and Technology of the Department of Homeland Security.

(7) An assessment of the interrelationship between the different university-based centers and the degree to which outreach and collaboration among a
diverse array of academic institutions is encouraged
by the Department of Homeland Security, particu-
larly with historically Black colleges and universities
and minority-serving institutions.

(8) A review of any other essential elements of
the programs determined in the conduct of the
study.

(c) INFORMATION RELATING TO UNIVERSITY-BASED
CENTERS.—Subparagraph (D) of section 308(b)(2) of the
Homeland Security Act of 2002 (6 U.S.C. 188(b)(2)) is
amended to read as follows:

“(D) ANNUAL REPORT TO CONGRESS.—
Not later than 1 year after the date of the en-
actment of this subparagraph and annually
thereafter, the Secretary shall submit to Con-
gress a report on the implementation of this
section. Each such report shall—

“(i) indicate which center or centers
have been designated pursuant to this sec-
tion;

“(ii) describe how such designation or
designations enhance homeland security;

“(iii) provide information on any deci-
sions to revoke or modify such designation
or designations;
“(iv) describe research that has been
tasked and completed by each center that
has been designated during the preceding
year;

“(v) describe funding provided by the
Secretary for each center under clause (iv)
for that year; and

“(vi) describe plans for utilization of
each center or centers in the forthcoming
year.”.

○