117TH CONGRESS
1st Session
HOUSE OF REPRESENTATIVES
REPORT
117–85

PIPELINE SECURITY ACT

JULY 13, 2021.—Committed to the Committee of the Whole House on the State of the Union and ordered to be printed

Mr. THOMPSON of Mississippi, from the Committee on Homeland Security, submitted the following

R E P O R T

[To accompany H.R. 3243]

The Committee on Homeland Security, to whom was referred the bill (H.R. 3243) to codify the Transportation Security Administration's responsibility relating to securing pipelines against cybersecurity threats, acts of terrorism, and other nefarious acts that jeopardize the physical security or cybersecurity of pipelines, and for other purposes, having considered the same, reports favorably thereon with amendments and recommends that the bill as amended do pass.

CONTENTS

The amendments (stated in terms of the introduced bill) are as follows:

Strike "pipeline security section" each place such term appears (including in any headings and in the amendment to the item relat-

ing to section 1631 added to the table of sections) and insert "pipeline security division".

Page 3, line 7, strike "section" and insert "division".

Page 3, line 21, strike "section" and insert "division".

Page 3, line 21, insert "in the executive service of the Administration" after "individual".

Page 3, line 24, strike "section"and insert "division".

Page 4, line 1, strike "section" and insert "division".

Page 4, line 2, strike "section" and insert "division".

Page 4, line 22, insert before the period the following: ", unless such guidelines are superseded by directives or regulations".

Page 5, beginning line 5, strike "to provide recommendations" and insert ", or mandatory security assessments if required by superseding directives or regulations, to provide recommendations or requirements".

Page 5, line 18, insert before the period the following: "or superseding directives or regulations".

Page 5, strike lines 19 through 21 and insert the following:

> "(6) Supporting the development and implementation of a security directive or regulation when the Administrator issues such a directive or regulation.

Page 5, line 22, strike "section's" and insert "division's".

Page 6, line 11, insert before the period the following: ", except to the extent such guidelines have been superseded by directives or regulations".

Page 7, after line 24, insert the following (and redesignate subsequent subsections accordingly):

> (c) CYBERSECURITY EXPERTISE.—The strategy shall include an assessment of the cybersecurity expertise determined necessary by the Administrator of the Transportation Security Administration and a plan for developing such expertise within the Administration.

Page 8, line 18, insert "directives, regulations," after "guidelines,".

PURPOSE AND SUMMARY

H.R. 3243, the "Pipeline Security Act," seeks to enhance the cybersecurity and physical security of our Nation's pipeline infrastructure by clarifying the Transportation Security Administration's (TSA) responsibility related to securing pipelines against cybersecurity threats, acts of terrorism, and other nefarious acts. The bill also sets requirements for a pipeline security division within TSA to help carry out this mission. Under this bill, TSA's pipeline security division must develop guidelines for pipeline security, conduct inspections of pipelines and pipeline facilities, and assist with the development and implementation of security directives and regulations related to pipeline security. In addition, the bill requires TSA and the Cybersecurity and Infrastructure Security Agency (CISA) to coordinate and develop a pipeline security personnel strategy to ensure TSA maintains appropriate pipeline security staffing and cybersecurity expertise. Finally, the bill requires TSA

to annually report to Congress regarding pipeline security, instructs the Government Accountability Office (GAO) to conduct a review of the implementation of this Act, and enhances TSA's engagement with pipeline security stakeholders.

BACKGROUND AND NEED FOR LEGISLATION

Since its establishment in 2001, pipeline security has been a part of TSA's mission to secure all modes of transportation, as pipelines have long been defined in law as a mode of transportation. To carry out this mission, TSA also has authority to promulgate mandatory security directives and regulations related to pipeline security, as it did on May 27, 2021, when it issued a security directive requiring pipeline operators to report cybersecurity incidents, designate incident response coordinators, and assess compliance with TSA security guidance.

Recently, the vulnerability of the Nation's oil and natural gas infrastructure was brought into sharp focus when, in May 2021, the Nation's largest fuel pipeline operator was the victim of a ransomware attack that caused a 6-day shutdown of the pipeline. The ransomware attack on the Colonial Pipeline Company resulted in communities across the East Coast experiencing extreme gasoline shortages and highlighted the importance of enhancing the cybersecurity and physical security of pipeline systems as well as the regulatory framework for protecting such systems.

H.R. 3243 builds upon TSA's existing statutory authority to secure pipelines to enhance efforts to address the evolving threat landscape. Under this legislation, TSA's pipeline security functions will be housed within a dedicated pipeline security division with senior-level leadership and personnel with cybersecurity expertise. Among its key functions, the pipeline security division would be charged with developing and maintaining guidelines for pipeline security and conducting inspections and risk assessments. The division would also assist with the development and implementation of security directives and regulations related to pipeline security, including forthcoming directives announced by the Secretary of Homeland Security on May 27, 2021.

As illustrated by the May 2021 Colonial Pipeline attack, the need for the Federal government to raise the bar on cybersecurity among pipeline operators is particularly acute. TSA, as a component of the Department of Homeland Security (DHS), is ideally positioned to coordinate with CISA, which has significant cybersecurity expertise. Further, TSA's position within DHS also ensures it has access to key Federal resources and intelligence related to physical threats against pipelines. H.R. 3243 facilitates intradepartmental collaboration by instructing TSA, in coordination with CISA, to develop a personnel strategy for the pipeline security division. This strategy is specifically required to include a plan for developing and maintaining appropriate cybersecurity expertise within TSA.

Finally, H.R. 3243 contains important oversight provisions regarding TSA's pipeline security efforts. It requires TSA to conduct additional stakeholder engagement, establishes annual pipeline security report requirements for TSA, and provides GAO with a mandate to review the legislation's implementation.

HEARINGS

For the purposes of clause 3(c)(6) of rule XIII, the following hearing was used to develop H.R. 3243:

The Committee did not hold a legislative hearing on H.R. 3243 in the 117th Congress. The legislation was informed by a hearing held in the 116th Congress. On February 22, 2019, the Subcommittee on Transportation and Maritime Security and the Subcommittee on Cybersecurity, Infrastructure Protection, and Innovation held a hearing entitled "Securing U.S. Surface Transportation from Cyber Attacks." The Subcommittees received testimony from Sonya Proctor, Director for the Surface Division, Office of Security Policy and Industry Engagement, TSA; Bob Kolasky, Director of National Risk Management Center, CISA; James Lewis, Senior Vice President and Director, Technology Policy Program, Center for Strategic & International Studies; Rebeca Gagliostro, Director of Security, Reliability, and Resilience, Interstate Natural Gas Association of America; Erik Olson, Vice President, Rail Security Alliance; and John Hultquist, Director of Intelligence Analysis, FireEye.

COMMITTEE CONSIDERATION

The Committee met on May 18, 2021, with a quorum being present, to consider H.R. 3243 and ordered the measure to be reported to the House with a favorable recommendation, with amendments, by unanimous consent.

COMMITTEE VOTES

Clause 3(b) of rule XIII of the Rules of the House of Representatives requires the Committee to list the recorded votes on the motion to report legislation and amendments thereto.

No recorded votes were requested during consideration of H.R. 3243.

COMMITTEE OVERSIGHT FINDINGS

In compliance with clause 3(c)(1) of rule XIII of the Rules of the House of Representatives, the Committee advises that the findings and recommendations of the Committee, based on oversight activities under clause 2(b)(1) of rule X of the Rules of the House of Representatives, are incorporated in the descriptive portions of this report.

CONGRESSIONAL BUDGET OFFICE ESTIMATE, NEW BUDGET AUTHORITY, ENTITLEMENT AUTHORITY, AND TAX EXPENDITURES

With respect to the requirements of clause 3(c)(2) of rule XIII of the Rules of the House of Representatives and section 308(a) of the Congressional Budget Act of 1974, and with respect to the requirements of clause 3(c)(3) of rule XIII of the Rules of the House of Representatives and section 402 of the Congressional Budget Act of 1974, the Committee has requested but not received from the Director of the Congressional Budget Office a statement as to whether this bill contains any new budget authority, spending authority, credit authority, or an increase or decrease in revenues or tax expenditures.

FEDERAL MANDATES STATEMENT

An estimate of Federal mandates prepared by the Director of the Congressional Budget Office pursuant to section 423 of the Unfunded Mandates Reform Act was not made available to the Committee in time for the filing of this report. The Chairman of the Committee shall cause such estimate to be printed in the Congressional Record upon its receipt by the Committee.

DUPLICATIVE FEDERAL PROGRAMS

Pursuant to clause 3(c) of rule XIII, the Committee finds that H.R. 3243 does not contain any provision that establishes or reauthorizes a program known to be duplicative of another Federal program.

STATEMENT OF GENERAL PERFORMANCE GOALS AND OBJECTIVES

Pursuant to clause 3(c)(4) of rule XIII of the Rules of the House of Representatives, the objectives of H.R. 3243 are to clarify TSA's pipeline security responsibilities and bolster its activities related to securing pipelines against cybersecurity threats, acts of terrorism, and other nefarious acts that jeopardize the cybersecurity or physical security of pipelines.

CONGRESSIONAL EARMARKS, LIMITED TAX BENEFITS, AND LIMITED TARIFF BENEFITS ADVISORY COMMITTEE STATEMENT

In compliance with rule XXI of the Rules of the House of Representatives, this bill, as reported, contains no congressional earmarks, limited tax benefits, or limited tariff benefits as defined in clause 9(d), 9(e), or 9(f) of the rule XXI.

APPLICABILITY TO LEGISLATIVE BRANCH

The Committee finds that H.R. 3243 does not relate to the terms and conditions of employment or access to public services or accommodations within the meaning of section 102(b)(3) of the Congressional Accountability Act.

SECTION-BY-SECTION ANALYSIS OF THE LEGISLATION

Section 1. Short Title.

This section provides that this bill may be cited as the "Pipeline Security Act."

Sec. 2. Pipeline Security Responsibilities.

This section amends subsection (f) of section 114 of title 49, United States Code, to add a new paragraph directing that the TSA Administrator, in coordination with the CISA Director, maintain responsibility relating to securing pipeline transportation and pipeline facilities against cybersecurity threats, acts of terrorism, and other nefarious acts that jeopardize the physical security or cybersecurity of pipeline transportation or facilities. The Committee believes that incorporating language calling on TSA to coordinate with CISA, an entity that was not established as a DHS component until 2018, uniquely positions TSA to carry out its pipeline security mission in the evolving threat landscape.

Sec. 3. Pipeline Security Division.

This section amends title XVI of the Homeland Security Act of 2002 by establishing a pipeline security division within TSA to carry out pipeline security programs. The mission of the pipeline security division is to oversee, in coordination with CISA, the security of pipeline transportation and pipeline facilities against cybersecurity threats, acts of terrorism, and other nefarious acts that jeopardize the physical security or cybersecurity of such transportation or facilities.

Additionally, this section requires the TSA Administrator to appoint a division head to the pipeline security division who has pipeline industry and security expertise. This individual must be in the executive service of TSA. This section further specifies that the division will be staffed by a workforce that includes personnel with cybersecurity expertise.

This section also articulates certain responsibilities of the pipeline security division. These responsibilities include developing guidelines for the physical security and cybersecurity of pipeline transportation and pipeline facilities, in coordination with relevant government, public, and private sector stakeholders. These guidelines must be updated based on intelligence and risk assessments no less than every three years and shared, as appropriate, with key pipeline security stakeholders, unless they are superseded by mandatory security directives or regulations. The division is further instructed to conduct cybersecurity and physical security assessments of pipelines to ensure voluntary compliance with these security guidelines and, as applicable, mandated compliance with security directives or regulations related to pipeline security. Other responsibilities of the division include carrying out a program to inspect pipelines and pipeline facilities, including inspections of pipeline facilities determined to be critical. The division is also tasked with supporting the development and implementation of security directives and regulations related to pipeline security.

Furthermore, the TSA Administrator and CISA Director are authorized to detail personnel between their components under this section. The pipeline security division will also be required to publish updated security guidelines within one year of the date of enactment, except if such guidelines have been superseded by security directives or regulations.

The Committee believes that establishing a division within TSA that is dedicated to pipeline security will enhance TSA's execution of its pipeline security mission by ensuring this mission receives senior-level leadership, personnel, and institutional visibility commensurate with its importance. Additionally, the Committee believes that by specifically articulating key responsibilities and authorities of this division, TSA will be able to more effectively engage with pipeline security stakeholders and assist with the development and implementation of guidance, security directives, and regulations on such matters. The Committee also believes that requiring a program to inspect critical pipelines and pipeline facilities is key to ensuring pipelines and pipeline facilities continually meet security standards. Finally, the Committee believes that authorizing the TSA Administrator and CISA Director to detail personnel between their components will help drive interagency com-

munication and collaboration and ensure DHS leverages the expertise of its different components effectively.

Sec. 4. Personnel Strategy.

This section requires TSA, in coordination with CISA, to develop a personnel strategy for the staffing of the pipeline security division within 180 days of the date of enactment. Upon development of the strategy, the TSA Administrator must provide the Committee on Homeland Security of the House of Representatives and the Committee on Commerce, Science, and Transportation of the Senate with a copy of such a strategy. The strategy must take into consideration the most recently published versions of key DHS and TSA strategy documents. Additionally, it must contain an assessment of the resources needed to carry out the pipeline security division's responsibilities and an assessment of TSA's pipeline security cybersecurity expertise, including a plan to further develop such expertise.

The Committee believes the development of a personnel strategy for the staffing of the pipeline security division will help TSA build upon its ongoing efforts to develop a workforce capable of ensuring the security of the pipeline sector, and that specifically assessing the need for cybersecurity expertise will help TSA acquire the workforce needed to counter current threats.

Sec. 5. Oversight.

This section requires the TSA Administrator to report to the Committee on Homeland Security of the House of Representatives and the Committee on Commerce, Science, and Transportation of the Senate about the activities of the pipeline security division, including information with respect to guidelines, security directives, regulations, security assessments, and inspections, no less than annually. Each report must include a determination by the Administrator regarding whether a need exists for additional regulations or non-regulatory initiatives and provide a justification for such determination.

Finally, the section requires GAO to conduct a review of the implementation of the Act, not later than two years after the date of enactment.

The Committee believes the requirements for regular reports to Congress and a GAO review will assist Congress in conducting effective oversight of TSA's pipeline security efforts. Such oversight will be key to ensuring the success of the pipeline security division.

Sec. 6. Stakeholder Engagement.

This section requires the TSA Administrator to convene not less than two industry days to engage with pipeline transportation and pipeline facilities stakeholders. These industry days shall occur not later than one year after the date of enactment.

The Committee has heard from pipeline stakeholders regarding the importance of information-sharing between the government and the private sector, as well as about the value of TSA's pipeline security capabilities in particular. Stakeholders have also noted that, during critical incidents, it is essential to have established lines of communication with key regulators. The Committee believes that the combination of a standing division dedicated to pipeline secu-

rity and requirements for meetings will enhance engagement between TSA and pipeline operators.

CHANGES IN EXISTING LAW MADE BY THE BILL, AS REPORTED

In compliance with clause 3(e) of rule XIII of the Rules of the House of Representatives, changes in existing law made by the bill, as reported, are shown as follows (existing law proposed to be omitted is enclosed in black brackets, new matter is printed in italics, and existing law in which no change is proposed is shown in roman):

TITLE 49, UNITED STATES CODE

* * * * * * *

SUBTITLE I—DEPARTMENT OF TRANSPORTATION

* * * * * * *

CHAPTER 1—ORGANIZATION

* * * * * * *

§ 114. Transportation Security Administration

(a) IN GENERAL.—The Transportation Security Administration shall be an administration of the Department of Homeland Security.

(b) LEADERSHIP.—

(1) HEAD OF TRANSPORTATION SECURITY ADMINISTRATION.—

(A) APPOINTMENT.—The head of the Administration shall be the Administrator of the Transportation Security Administration (referred to in this section as the "Administrator"). The Administrator shall be appointed by the President, by and with the advice and consent of the Senate.

(B) QUALIFICATIONS.—The Administrator must—

(i) be a citizen of the United States; and

(ii) have experience in a field directly related to transportation or security.

(C) TERM.—Effective with respect to any individual appointment by the President, by and with the advice and consent of the Senate, after the date of enactment of the TSA Modernization Act, the term of office of an individual appointed as the Administrator shall be 5 years. The term of office of an individual serving as the Administrator on the date of enactment of the TSA Modernization Act shall be 5 years beginning on the date that the Administrator began serving.

(2) DEPUTY ADMINISTRATOR.—

(A) APPOINTMENT.—There is established in the Transportation Security Administration a Deputy Administrator, who shall assist the Administrator in the management of the Transportation Security Administration. The Deputy Administrator shall be appointed by the President.

(B) VACANCY.—The Deputy Administrator shall be Acting Administrator during the absence or incapacity of the Administrator or during a vacancy in the office of Administrator.

(C) QUALIFICATIONS.—The Deputy Administrator must—

(i) be a citizen of the United States; and

(ii) have experience in a field directly related to transportation or security.

(3) CHIEF COUNSEL.—

(A) APPOINTMENT.—There is established in the Transportation Security Administration a Chief Counsel, who shall advise the Administrator and other senior officials on all legal matters relating to the responsibilities, functions, and management of the Transportation Security Administration.

(B) QUALIFICATIONS.—The Chief Counsel must be a citizen of the United States.

(c) LIMITATION ON OWNERSHIP OF STOCKS AND BONDS.—The Administrator may not own stock in or bonds of a transportation or security enterprise or an enterprise that makes equipment that could be used for security purposes.

(d) FUNCTIONS.—The Administrator shall be responsible for security in all modes of transportation, including—

(1) carrying out chapter 449, relating to civil aviation security, and related research and development activities; and

(2) security responsibilities over other modes of transportation that are exercised by the Department of Transportation.

(e) SCREENING OPERATIONS.—The Administrator shall—

(1) be responsible for day-to-day Federal security screening operations for passenger air transportation and intrastate air transportation under sections 44901 and 44935;

(2) develop standards for the hiring and retention of security screening personnel;

(3) train and test security screening personnel; and

(4) be responsible for hiring and training personnel to provide security screening at all airports in the United States where screening is required under section 44901, in consultation with the Secretary of Transportation and the heads of other appropriate Federal agencies and departments.

(f) ADDITIONAL DUTIES AND POWERS.—In addition to carrying out the functions specified in subsections (d) and (e), the Administrator shall—

(1) receive, assess, and distribute intelligence information related to transportation security;

(2) assess threats to transportation;

(3) develop policies, strategies, and plans for dealing with threats to transportation security;

(4) make other plans related to transportation security, including coordinating countermeasures with appropriate departments, agencies, and instrumentalities of the United States Government;

(5) serve as the primary liaison for transportation security to the intelligence and law enforcement communities;

(6) on a day-to-day basis, manage and provide operational guidance to the field security resources of the Administration,

including Federal Security Managers as provided by section 44933;

(7) enforce security-related regulations and requirements;

(8) identify and undertake research and development activities necessary to enhance transportation security;

(9) inspect, maintain, and test security facilities, equipment, and systems;

(10) ensure the adequacy of security measures for the transportation of cargo;

(11) oversee the implementation, and ensure the adequacy, of security measures at airports and other transportation facilities;

(12) require background checks for airport security screening personnel, individuals with access to secure areas of airports, and other transportation security personnel;

(13) work in conjunction with the Administrator of the Federal Aviation Administration with respect to any actions or activities that may affect aviation safety or air carrier operations;

(14) work with the International Civil Aviation Organization and appropriate aeronautic authorities of foreign governments under section 44907 to address security concerns on passenger flights by foreign air carriers in foreign air transportation;

(15) establish and maintain a National Deployment Office as required under section 44948 of this title; [and]

(16) maintain responsibility, in coordination with the Director of the Cybersecurity and Infrastructure Security Agency, as appropriate, relating to securing pipeline transportation and pipeline facilities (as such terms are defined in section 60101 of this title) against cybersecurity threats (as such term is defined in section 102 of the Cybersecurity Information Sharing Act of 2015 (Public Law 114–113; 6 U.S.C. 1501)), an act of terrorism (as such term is defined in section 3077 of title 18), and other nefarious acts that jeopardize the physical security or cybersecurity of such transportation or facilities; and

[(16)] *(17)* carry out such other duties, and exercise such other powers, relating to transportation security as the Administrator considers appropriate, to the extent authorized by law.

(g) NATIONAL EMERGENCY RESPONSIBILITIES.—

(1) IN GENERAL.—Subject to the direction and control of the Secretary of Homeland Security, the Administrator, during a national emergency, shall have the following responsibilities:

(A) To coordinate domestic transportation, including aviation, rail, and other surface transportation, and maritime transportation (including port security).

(B) To coordinate and oversee the transportation-related responsibilities of other departments and agencies of the Federal Government other than the Department of Defense and the military departments.

(C) To coordinate and provide notice to other departments and agencies of the Federal Government, and appropriate agencies of State and local governments, including departments and agencies for transportation, law enforcement, and border control, about threats to transportation.

(D) To carry out such other duties, and exercise such other powers, relating to transportation during a national emergency as the Secretary of Homeland Security shall prescribe.

(2) AUTHORITY OF OTHER DEPARTMENTS AND AGENCIES.—The authority of the Administrator under this subsection shall not supersede the authority of any other department or agency of the Federal Government under law with respect to transportation or transportation-related matters, whether or not during a national emergency.

(3) CIRCUMSTANCES.—The Secretary of Homeland Security shall prescribe the circumstances constituting a national emergency for purposes of this subsection.

(h) MANAGEMENT OF SECURITY INFORMATION.—In consultation with the Transportation Security Oversight Board, the Administrator shall—

(1) enter into memoranda of understanding with Federal agencies or other entities to share or otherwise cross-check as necessary data on individuals identified on Federal agency databases who may pose a risk to transportation or national security;

(2) establish procedures for notifying the Administrator of the Federal Aviation Administration, appropriate State and local law enforcement officials, and airport or airline security officers of the identity of individuals known to pose, or suspected of posing, a risk of air piracy or terrorism or a threat to airline or passenger safety;

(3) in consultation with other appropriate Federal agencies and air carriers, establish policies and procedures requiring air carriers—

(A) to use information from government agencies to identify individuals on passenger lists who may be a threat to civil aviation or national security; and

(B) if such an individual is identified, notify appropriate law enforcement agencies, prevent the individual from boarding an aircraft, or take other appropriate action with respect to that individual; and

(4) consider requiring passenger air carriers to share passenger lists with appropriate Federal agencies for the purpose of identifying individuals who may pose a threat to aviation safety or national security.

(i) VIEW OF NTSB.—In taking any action under this section that could affect safety, the Administrator shall give great weight to the timely views of the National Transportation Safety Board.

(j) ACQUISITIONS.—

(1) IN GENERAL.—The Administrator is authorized—

(A) to acquire (by purchase, lease, condemnation, or otherwise) such real property, or any interest therein, within and outside the continental United States, as the Administrator considers necessary;

(B) to acquire (by purchase, lease, condemnation, or otherwise) and to construct, repair, operate, and maintain such personal property (including office space and patents), or any interest therein, within and outside the conti-

nental United States, as the Administrator considers necessary;

(C) to lease to others such real and personal property and to provide by contract or otherwise for necessary facilities for the welfare of its employees and to acquire, maintain, and operate equipment for these facilities;

(D) to acquire services, including such personal services as the Secretary of Homeland Security determines necessary, and to acquire (by purchase, lease, condemnation, or otherwise) and to construct, repair, operate, and maintain research and testing sites and facilities; and

(E) in cooperation with the Administrator of the Federal Aviation Administration, to utilize the research and development facilities of the Federal Aviation Administration.

(2) TITLE.—Title to any property or interest therein acquired pursuant to this subsection shall be held by the Government of the United States.

(k) TRANSFERS OF FUNDS.—The Administrator is authorized to accept transfers of unobligated balances and unexpended balances of funds appropriated to other Federal agencies (as such term is defined in section 551(1) of title 5) to carry out functions assigned by law to the Administrator.

(l) REGULATIONS.—

(1) IN GENERAL.—The Administrator is authorized to issue, rescind, and revise such regulations as are necessary to carry out the functions of the Administration.

(2) EMERGENCY PROCEDURES.—

(A) IN GENERAL.—Notwithstanding any other provision of law or executive order (including an executive order requiring a cost-benefit analysis), if the Administrator determines that a regulation or security directive must be issued immediately in order to protect transportation security, the Administrator shall issue the regulation or security directive without providing notice or an opportunity for comment and without prior approval of the Secretary.

(B) REVIEW BY TRANSPORTATION SECURITY OVERSIGHT BOARD.—Any regulation or security directive issued under this paragraph shall be subject to review by the Transportation Security Oversight Board established under section 115. Any regulation or security directive issued under this paragraph shall remain effective for a period not to exceed 90 days unless ratified or disapproved by the Board or rescinded by the Administrator.

(3) FACTORS TO CONSIDER.—In determining whether to issue, rescind, or revise a regulation under this section, the Administrator shall consider, as a factor in the final determination, whether the costs of the regulation are excessive in relation to the enhancement of security the regulation will provide. The Administrator may waive requirements for an analysis that estimates the number of lives that will be saved by the regulation and the monetary value of such lives if the Administrator determines that it is not feasible to make such an estimate.

(4) AIRWORTHINESS OBJECTIONS BY FAA.—

(A) IN GENERAL.—The Administrator shall not take an aviation security action under this title if the Adminis-

trator of the Federal Aviation Administration notifies the Administrator that the action could adversely affect the airworthiness of an aircraft.

(B) REVIEW BY SECRETARY.—Notwithstanding subparagraph (A), the Administrator may take such an action, after receiving a notification concerning the action from the Administrator of the Federal Aviation Administration under subparagraph (A), if the Secretary of Transportation subsequently approves the action.

(m) PERSONNEL AND SERVICES; COOPERATION BY ADMINISTRATOR.—

(1) AUTHORITY OF ADMINISTRATOR.—In carrying out the functions of the Administration, the Administrator shall have the same authority as is provided to the Administrator of the Federal Aviation Administration under subsections (*l*) and (m) of section 106.

(2) AUTHORITY OF AGENCY HEADS.—The head of a Federal agency shall have the same authority to provide services, supplies, equipment, personnel, and facilities to the Administrator as the head has to provide services, supplies, equipment, personnel, and facilities to the Administrator of the Federal Aviation Administration under section 106(m).

(n) PERSONNEL MANAGEMENT SYSTEM.—

(1) IN GENERAL.—The personnel management system established by the Administrator of the Federal Aviation Administration under section 40122 shall apply to employees of the Transportation Security Administration, or, subject to the requirements of such section, the Administrator may make such modifications to the personnel management system with respect to such employees as the Administrator considers appropriate, such as adopting aspects of other personnel systems of the Department of Homeland Security.

(2) MERITORIOUS EXECUTIVE OR DISTINGUISHED EXECUTIVE RANK AWARDS.—Notwithstanding section 40122(g)(2) of this title, the applicable sections of title 5 shall apply to the Transportation Security Administration personnel management system, except that—

(A) for purposes of applying such provisions to the personnel management system—

(i) the term "agency" means the Department of Homeland Security;

(ii) the term "senior executive" means a Transportation Security Administration executive serving on a Transportation Security Executive Service appointment;

(iii) the term "career appointee" means a Transportation Security Administration executive serving on a career Transportation Security Executive Service appointment; and

(iv) The term "senior career employee" means a Transportation Security Administration employee covered by the Transportation Security Administration Core Compensation System at the L or M pay band;

(B) receipt by a career appointee or a senior career employee of the rank of Meritorious Executive or Meritorious

Senior Professional entitles the individual to a lump-sum payment of an amount equal to 20 percent of annual basic pay, which shall be in addition to the basic pay paid under the applicable Transportation Security Administration pay system; and

(C) receipt by a career appointee or a senior career employee of the rank of Distinguished Executive or Distinguished Senior Professional entitles the individual to a lump-sum payment of an amount equal to 35 percent of annual basic pay, which shall be in addition to the basic pay paid under the applicable Transportation Security Administration pay system.

(3) DEFINITION OF APPLICABLE SECTIONS OF TITLE 5.—In this subsection, the term "applicable sections of title 5" means—

(A) subsections (b), (c) and (d) of section 4507 of title 5; and

(B) subsections (b) and (c) of section 4507a of title 5.

(o) AUTHORITY OF INSPECTOR GENERAL.—The Transportation Security Administration shall be subject to the Inspector General Act of 1978 (5 U.S.C. App.) and other laws relating to the authority of the Inspector General of the Department of Homeland Security.

(p) LAW ENFORCEMENT POWERS.—

(1) IN GENERAL.—The Administrator may designate an employee of the Transportation Security Administration or other Federal agency to serve as a law enforcement officer.

(2) POWERS.—While engaged in official duties of the Administration as required to fulfill the responsibilities under this section, a law enforcement officer designated under paragraph (1) may—

(A) carry a firearm;

(B) make an arrest without a warrant for any offense against the United States committed in the presence of the officer, or for any felony cognizable under the laws of the United States if the officer has probable cause to believe that the person to be arrested has committed or is committing the felony; and

(C) seek and execute warrants for arrest or seizure of evidence issued under the authority of the United States upon probable cause that a violation has been committed.

(3) GUIDELINES ON EXERCISE OF AUTHORITY.—The authority provided by this subsection shall be exercised in accordance with guidelines prescribed by the Administrator, in consultation with the Attorney General of the United States, and shall include adherence to the Attorney General's policy on use of deadly force.

(4) REVOCATION OR SUSPENSION OF AUTHORITY.—The powers authorized by this subsection may be rescinded or suspended should the Attorney General determine that the Administrator has not complied with the guidelines prescribed in paragraph (3) and conveys the determination in writing to the Secretary of Homeland Security and the Administrator.

(q) AUTHORITY TO EXEMPT.—The Administrator may grant an exemption from a regulation prescribed in carrying out this section if the Administrator determines that the exemption is in the public interest.

(r) NONDISCLOSURE OF SECURITY ACTIVITIES.—

(1) IN GENERAL.—Notwithstanding section 552 of title 5, the Administrator shall prescribe regulations prohibiting the disclosure of information obtained or developed in carrying out security under authority of the Aviation and Transportation Security Act (Public Law 107–71) or under chapter 449 of this title if the Administrator decides that disclosing the information would—

(A) be an unwarranted invasion of personal privacy;

(B) reveal a trade secret or privileged or confidential commercial or financial information; or

(C) be detrimental to the security of transportation.

(2) AVAILABILITY OF INFORMATION TO CONGRESS.—Paragraph (1) does not authorize information to be withheld from a committee of Congress authorized to have the information.

(3) LIMITATION ON TRANSFERABILITY OF DUTIES.—Except as otherwise provided by law, the Administrator may not transfer a duty or power under this subsection to another department, agency, or instrumentality of the United States.

(4) LIMITATIONS.—Nothing in this subsection, or any other provision of law, shall be construed to authorize the designation of information as sensitive security information (as defined in section 1520.5 of title 49, Code of Federal Regulations)—

(A) to conceal a violation of law, inefficiency, or administrative error;

(B) to prevent embarrassment to a person, organization, or agency;

(C) to restrain competition; or

(D) to prevent or delay the release of information that does not require protection in the interest of transportation security, including basic scientific research information not clearly related to transportation security.

(s) TRANSPORTATION SECURITY STRATEGIC PLANNING.—

(1) IN GENERAL.—The Secretary of Homeland Security shall develop, prepare, implement, and update, as needed—

(A) a National Strategy for Transportation Security; and

(B) transportation modal security plans addressing security risks, including threats, vulnerabilities, and consequences, for aviation, railroad, ferry, highway, maritime, pipeline, public transportation, over-the-road bus, and other transportation infrastructure assets.

(2) ROLE OF SECRETARY OF TRANSPORTATION.—The Secretary of Homeland Security shall work jointly with the Secretary of Transportation in developing, revising, and updating the documents required by paragraph (1).

(3) CONTENTS OF NATIONAL STRATEGY FOR TRANSPORTATION SECURITY.—The National Strategy for Transportation Security shall include the following:

(A) An identification and evaluation of the transportation assets in the United States that, in the interests of national security and commerce, must be protected from attack or disruption by terrorist or other hostile forces, including modal security plans for aviation, bridge and tunnel, commuter rail and ferry, highway, maritime, pipeline, rail, mass transit, over-the-road bus, and other public

transportation infrastructure assets that could be at risk of such an attack or disruption.

(B) The development of risk-based priorities, based on risk assessments conducted or received by the Secretary of Homeland Security (including assessments conducted under the Implementing Recommendations of the 9/11 Commission Act of 2007) across all transportation modes and realistic deadlines for addressing security needs associated with those assets referred to in subparagraph (A).

(C) The most appropriate, practical, and cost-effective means of defending those assets against threats to their security.

(D) A forward-looking strategic plan that sets forth the agreed upon roles and missions of Federal, State, regional, local, and tribal authorities and establishes mechanisms for encouraging cooperation and participation by private sector entities, including nonprofit employee labor organizations, in the implementation of such plan.

(E) A comprehensive delineation of prevention, response, and recovery responsibilities and issues regarding threatened and executed acts of terrorism within the United States and threatened and executed acts of terrorism outside the United States to the extent such acts affect United States transportation systems.

(F) A prioritization of research and development objectives that support transportation security needs, giving a higher priority to research and development directed toward protecting vital transportation assets. Transportation security research and development projects shall be based, to the extent practicable, on such prioritization. Nothing in the preceding sentence shall be construed to require the termination of any research or development project initiated by the Secretary of Homeland Security or the Secretary of Transportation before the date of enactment of the Implementing Recommendations of the 9/11 Commission Act of 2007.

(G) A 3- and 10-year budget for Federal transportation security programs that will achieve the priorities of the National Strategy for Transportation Security.

(H) Methods for linking the individual transportation modal security plans and the programs contained therein, and a plan for addressing the security needs of intermodal transportation.

(I) Transportation modal security plans described in paragraph (1)(B), including operational recovery plans to expedite, to the maximum extent practicable, the return to operation of an adversely affected transportation system following a major terrorist attack on that system or other incident. These plans shall be coordinated with the resumption of trade protocols required under section 202 of the SAFE Port Act (6 U.S.C. 942) and the National Maritime Transportation Security Plan required under section 70103(a) of title 46.

(4) SUBMISSION OF PLANS.—

(A) IN GENERAL.—The Secretary of Homeland Security shall submit the National Strategy for Transportation Security, including the transportation modal security plans and any revisions to the National Strategy for Transportation Security and the transportation modal security plans, to appropriate congressional committees not less frequently than April 1 of each even-numbered year.

(B) PERIODIC PROGRESS REPORT.—

(i) REQUIREMENT FOR REPORT.—Each year, in conjunction with the submission of the budget to Congress under section 1105(a) of title 31, United States Code, the Secretary of Homeland Security shall submit to the appropriate congressional committees an assessment of the progress made on implementing the National Strategy for Transportation Security, including the transportation modal security plans.

(ii) CONTENT.—Each progress report submitted under this subparagraph shall include, at a minimum, the following:

(I) Recommendations for improving and implementing the National Strategy for Transportation Security and the transportation modal and intermodal security plans that the Secretary of Homeland Security, in consultation with the Secretary of Transportation, considers appropriate.

(II) An accounting of all grants for transportation security, including grants and contracts for research and development, awarded by the Secretary of Homeland Security in the most recent fiscal year and a description of how such grants accomplished the goals of the National Strategy for Transportation Security.

(III) An accounting of all—

(aa) funds requested in the President's budget submitted pursuant to section 1105 of title 31 for the most recent fiscal year for transportation security, by mode;

(bb) personnel working on transportation security by mode, including the number of contractors; and

(cc) information on the turnover in the previous year among senior staff of the Department of Homeland Security, including component agencies, working on transportation security issues. Such information shall include the number of employees who have permanently left the office, agency, or area in which they worked, and the amount of time that they worked for the Department of Homeland Security.

(iii) WRITTEN EXPLANATION OF TRANSPORTATION SECURITY ACTIVITIES NOT DELINEATED IN THE NATIONAL STRATEGY FOR TRANSPORTATION SECURITY.—At the end of each fiscal year, the Secretary of Homeland Security shall submit to the appropriate congressional commit-

tees a written explanation of any Federal transportation security activity that is inconsistent with the National Strategy for Transportation Security, including the amount of funds to be expended for the activity and the number of personnel involved.

(C) CLASSIFIED MATERIAL.—Any part of the National Strategy for Transportation Security or the transportation modal security plans that involve information that is properly classified under criteria established by Executive order shall be submitted to the appropriate congressional committees separately in a classified format.

(D) APPROPRIATE CONGRESSIONAL COMMITTEES DEFINED.—In this subsection, the term "appropriate congressional committees" means the Committee on Transportation and Infrastructure and the Committee on Homeland Security of the House of Representatives and the Committee on Commerce, Science, and Transportation, the Committee on Homeland Security and Governmental Affairs, and the Committee on Banking, Housing, and Urban Affairs of the Senate.

(5) PRIORITY STATUS.—

(A) IN GENERAL.—The National Strategy for Transportation Security shall be the governing document for Federal transportation security efforts.

(B) OTHER PLANS AND REPORTS.—The National Strategy for Transportation Security shall include, as an integral part or as an appendix—

(i) the current National Maritime Transportation Security Plan under section 70103 of title 46;

(ii) the report required by section 44938 of this title;

(iii) transportation modal security plans required under this section;

(iv) the transportation sector specific plan required under Homeland Security Presidential Directive–7; and

(v) any other transportation security plan or report that the Secretary of Homeland Security determines appropriate for inclusion.

(6) COORDINATION.—In carrying out the responsibilities under this section, the Secretary of Homeland Security, in coordination with the Secretary of Transportation, shall consult, as appropriate, with Federal, State, and local agencies, tribal governments, private sector entities (including nonprofit employee labor organizations), institutions of higher learning, and other entities.

(7) PLAN DISTRIBUTION.—The Secretary of Homeland Security shall make available and appropriately publicize an unclassified version of the National Strategy for Transportation Security, including its component transportation modal security plans, to Federal, State, regional, local and tribal authorities, transportation system owners or operators, private sector stakeholders, including nonprofit employee labor organizations representing transportation employees, institutions of higher learning, and other appropriate entities.

(t) TRANSPORTATION SECURITY INFORMATION SHARING PLAN.—

(1) DEFINITIONS.—In this subsection:

(A) APPROPRIATE CONGRESSIONAL COMMITTEES.—The term "appropriate congressional committees" has the meaning given that term in subsection (s)(4)(E).

(B) PLAN.—The term "Plan" means the Transportation Security Information Sharing Plan established under paragraph (2).

(C) PUBLIC AND PRIVATE STAKEHOLDERS.—The term "public and private stakeholders" means Federal, State, and local agencies, tribal governments, and appropriate private entities, including nonprofit employee labor organizations representing transportation employees.

(D) TRANSPORTATION SECURITY INFORMATION.—The term "transportation security information" means information relating to the risks to transportation modes, including aviation, public transportation, railroad, ferry, highway, maritime, pipeline, and over-the-road bus transportation, and may include specific and general intelligence products, as appropriate.

(2) ESTABLISHMENT OF PLAN.—The Secretary of Homeland Security, in consultation with the program manager of the information sharing environment established under section 1016 of the Intelligence Reform and Terrorism Prevention Act of 2004 (6 U.S.C. 485), the Secretary of Transportation, and public and private stakeholders, shall establish a Transportation Security Information Sharing Plan. In establishing the Plan, the Secretary of Homeland Security shall gather input on the development of the Plan from private and public stakeholders and the program manager of the information sharing environment established under section 1016 of the Intelligence Reform and Terrorism Prevention Act of 2004 (6 U.S.C. 485).

(3) PURPOSE OF PLAN.—The Plan shall promote sharing of transportation security information between the Department of Homeland Security and public and private stakeholders.

(4) CONTENT OF PLAN.—The Plan shall include—

(A) a description of how intelligence analysts within the Department of Homeland Security will coordinate their activities within the Department and with other Federal, State, and local agencies, and tribal governments, including coordination with existing modal information sharing centers and the center described in section 1410 of the Implementing Recommendations of the 9/11 Commission Act of 2007;

(B) the establishment of a point of contact, which may be a single point of contact within the Department of Homeland Security, for each mode of transportation for the sharing of transportation security information with public and private stakeholders, including an explanation and justification to the appropriate congressional committees if the point of contact established pursuant to this subparagraph differs from the agency within the Department of Homeland Security that has the primary authority, or has been delegated such authority by the Secretary of Homeland Security, to regulate the security of that transportation mode;

(C) a reasonable deadline by which the Plan will be implemented; and

(D) a description of resource needs for fulfilling the Plan.

(5) COORDINATION WITH INFORMATION SHARING.—The Plan shall be—

(A) implemented in coordination, as appropriate, with the program manager for the information sharing environment established under section 1016 of the Intelligence Reform and Terrorism Prevention Act of 2004 (6 U.S.C. 485); and

(B) consistent with the establishment of the information sharing environment and any policies, guidelines, procedures, instructions, or standards established by the President or the program manager for the implementation and management of the information sharing environment.

(6) ANNUAL REPORT ON PLAN.—The Secretary of Homeland Security shall annually submit to the appropriate congressional committees a report containing the Plan.

(7) SECURITY CLEARANCES.—The Secretary of Homeland Security shall, to the greatest extent practicable, take steps to expedite the security clearances needed for designated public and private stakeholders to receive and obtain access to classified information distributed under this section, as appropriate.

(8) CLASSIFICATION OF MATERIAL.—The Secretary of Homeland Security, to the greatest extent practicable, shall provide designated public and private stakeholders with transportation security information in an unclassified format.

(u) ENFORCEMENT OF REGULATIONS AND ORDERS OF THE SECRETARY OF HOMELAND SECURITY.—

(1) APPLICATION OF SUBSECTION.—

(A) IN GENERAL.—This subsection applies to the enforcement of regulations prescribed, and orders issued, by the Secretary of Homeland Security under a provision of chapter 701 of title 46 and under a provision of this title other than a provision of chapter 449 (in this subsection referred to as an "applicable provision of this title").

(B) VIOLATIONS OF CHAPTER 449.—The penalties for violations of regulations prescribed and orders issued by the Secretary of Homeland Security or the Administrator under chapter 449 of this title are provided under chapter 463 of this title.

(C) NONAPPLICATION TO CERTAIN VIOLATIONS.—

(i) Paragraphs (2) through (5) do not apply to violations of regulations prescribed, and orders issued, by the Secretary of Homeland Security under a provision of this title—

(I) involving the transportation of personnel or shipments of materials by contractors where the Department of Defense has assumed control and responsibility;

(II) by a member of the armed forces of the United States when performing official duties; or

(III) by a civilian employee of the Department of Defense when performing official duties.

(ii) Violations described in subclause (I), (II), or (III) of clause (i) shall be subject to penalties as determined by the Secretary of Defense or the Secretary of Defense's designee.

(2) CIVIL PENALTY.—

(A) IN GENERAL.—A person is liable to the United States Government for a civil penalty of not more than $10,000 for a violation of a regulation prescribed, or order issued, by the Secretary of Homeland Security under an applicable provision of this title.

(B) REPEAT VIOLATIONS.—A separate violation occurs under this paragraph for each day the violation continues.

(3) ADMINISTRATIVE IMPOSITION OF CIVIL PENALTIES.—

(A) IN GENERAL.—The Secretary of Homeland Security may impose a civil penalty for a violation of a regulation prescribed, or order issued, under an applicable provision of this title. The Secretary shall give written notice of the finding of a violation and the penalty.

(B) SCOPE OF CIVIL ACTION.—In a civil action to collect a civil penalty imposed by the Secretary of Homeland Security under this subsection, a court may not re-examine issues of liability or the amount of the penalty.

(C) JURISDICTION.—The district courts of the United States shall have exclusive jurisdiction of civil actions to collect a civil penalty imposed by the Secretary of Homeland Security under this subsection if—

(i) the amount in controversy is more than—

(I) $400,000, if the violation was committed by a person other than an individual or small business concern; or

(II) $50,000 if the violation was committed by an individual or small business concern;

(ii) the action is in rem or another action in rem based on the same violation has been brought; or

(iii) another action has been brought for an injunction based on the same violation.

(D) MAXIMUM PENALTY.—The maximum civil penalty the Secretary of Homeland Security administratively may impose under this paragraph is—

(i) $400,000, if the violation was committed by a person other than an individual or small business concern; or

(ii) $50,000, if the violation was committed by an individual or small business concern.

(E) NOTICE AND OPPORTUNITY TO REQUEST HEARING.—Before imposing a penalty under this section the Secretary of Homeland Security shall provide to the person against whom the penalty is to be imposed—

(i) written notice of the proposed penalty; and

(ii) the opportunity to request a hearing on the proposed penalty, if the Secretary of Homeland Security receives the request not later than 30 days after the date on which the person receives notice.

(4) COMPROMISE AND SETOFF.—

(A) The Secretary of Homeland Security may compromise the amount of a civil penalty imposed under this subsection.

(B) The Government may deduct the amount of a civil penalty imposed or compromised under this subsection from amounts it owes the person liable for the penalty.

(5) INVESTIGATIONS AND PROCEEDINGS.—Chapter 461 shall apply to investigations and proceedings brought under this subsection to the same extent that it applies to investigations and proceedings brought with respect to aviation security duties designated to be carried out by the Secretary of Homeland Security.

(6) DEFINITIONS.—In this subsection:

(A) PERSON.—The term "person" does not include—

(i) the United States Postal Service; or

(ii) the Department of Defense.

(B) SMALL BUSINESS CONCERN.—The term "small business concern" has the meaning given that term in section 3 of the Small Business Act (15 U.S.C. 632).

(7) ENFORCEMENT TRANSPARENCY.—

(A) IN GENERAL.—The Secretary of Homeland Security shall—

(i) provide an annual summary to the public of all enforcement actions taken by the Secretary under this subsection; and

(ii) include in each such summary the docket number of each enforcement action, the type of alleged violation, the penalty or penalties proposed, and the final assessment amount of each penalty.

(B) ELECTRONIC AVAILABILITY.—Each summary under this paragraph shall be made available to the public by electronic means.

(C) RELATIONSHIP TO THE FREEDOM OF INFORMATION ACT AND THE PRIVACY ACT.—Nothing in this subsection shall be construed to require disclosure of information or records that are exempt from disclosure under sections 552 or 552a of title 5.

(v) AUTHORIZATION OF APPROPRIATIONS.—There are authorized to be appropriated to the Transportation Security Administration for salaries, operations, and maintenance of the Administration—

(1) $7,849,247,000 for fiscal year 2019;

(2) $7,888,494,000 for fiscal year 2020; and

(3) $7,917,936,000 for fiscal year 2021.

(w) LEADERSHIP AND ORGANIZATION.—

(1) IN GENERAL.—For each of the areas described in paragraph (2), the Administrator of the Transportation Security Administration shall appoint at least 1 individual who shall—

(A) report directly to the Administrator or the Administrator's designated direct report; and

(B) be responsible and accountable for that area.

(2) AREAS DESCRIBED.—The areas described in this paragraph are as follows:

(A) Aviation security operations and training, including risk-based, adaptive security—

(i) focused on airport checkpoint and baggage screening operations;

(ii) workforce training and development programs; and

(iii) ensuring compliance with aviation security law, including regulations, and other specialized programs designed to secure air transportation.

(B) Surface transportation security operations and training, including risk-based, adaptive security—

(i) focused on accomplishing security systems assessments;

(ii) reviewing and prioritizing projects for appropriated surface transportation security grants;

(iii) operator compliance with surface transportation security law, including regulations, and voluntary industry standards; and

(iv) workforce training and development programs, and other specialized programs designed to secure surface transportation.

(C) Transportation industry engagement and planning, including the development, interpretation, promotion, and oversight of a unified effort regarding risk-based, risk-reducing security policies and plans (including strategic planning for future contingencies and security challenges) between government and transportation stakeholders, including airports, domestic and international airlines, general aviation, air cargo, mass transit and passenger rail, freight rail, pipeline, highway and motor carriers, and maritime.

(D) International strategy and operations, including agency efforts to work with international partners to secure the global transportation network.

(E) Trusted and registered traveler programs, including the management and marketing of the agency's trusted traveler initiatives, including the PreCheck Program, and coordination with trusted traveler programs of other Department of Homeland Security agencies and the private sector.

(F) Technology acquisition and deployment, including the oversight, development, testing, evaluation, acquisition, deployment, and maintenance of security technology and other acquisition programs.

(G) Inspection and compliance, including the integrity, efficiency and effectiveness of the agency's workforce, operations, and programs through objective audits, covert testing, inspections, criminal investigations, and regulatory compliance.

(H) Civil rights, liberties, and traveler engagement, including ensuring that agency employees and the traveling public are treated in a fair and lawful manner consistent with Federal laws and regulations protecting privacy and prohibiting discrimination and reprisal.

(I) Legislative and public affairs, including communication and engagement with internal and external audiences in a timely, accurate, and transparent manner, and devel-

opment and implementation of strategies within the agency to achieve congressional approval or authorization of agency programs and policies.

(3) NOTIFICATION.—The Administrator shall submit to the appropriate committees of Congress—

(A) not later than 180 days after the date of enactment of the TSA Modernization Act, a list of the names of the individuals appointed under paragraph (1); and

(B) an update of the list not later than 5 days after any new individual is appointed under paragraph (1).

* * * * * * *

HOMELAND SECURITY ACT OF 2002

SECTION 1. SHORT TITLE; TABLE OF CONTENTS.

(a) SHORT TITLE.—This Act may be cited as the "Homeland Security Act of 2002".

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

TITLE XVI—TRANSPORTATION SECURITY

* * * * * * *

Subtitle D—Pipeline Security

SEC. 1631. PIPELINE SECURITY DIVISION.

(a) ESTABLISHMENT.—There is within the Administration a pipeline security division to carry out pipeline security programs in furtherance of section 114(f)(16) of title 49, United States Code.

(b) MISSION.—The mission of the division referred to in subsection (a) is to oversee, in coordination with the Cybersecurity and Infrastructure Security Agency of the Department, the security of pipeline transportation and pipeline facilities (as such terms are defined in section 60101 of title 49, United States Code) against cybersecurity threats (as such term is defined in section 102 of the Cybersecurity Information Sharing Act of 2015 (Public Law 114–113; 6 U.S.C. 1501)), an act of terrorism (as such term is defined in section 3077 of title 18, United States Code), and other nefarious acts that jeopardize the physical security or cybersecurity of such transportation or facilities.

(c) LEADERSHIP; STAFFING.—The Administrator shall appoint as the head of the division an individual in the executive service of the Administration with knowledge of the pipeline industry and security best practices, as determined appropriate by the Administrator. The division shall be staffed by a workforce that includes personnel with cybersecurity expertise.

(d) RESPONSIBILITIES.—The division shall be responsible for carrying out the duties of the division as directed by the Administrator, acting through the head appointed pursuant to subsection (c). Such duties shall include the following:

(1) Developing, in consultation with relevant Federal, State, local, Tribal, and territorial entities and public and private sector stakeholders, guidelines for improving the security of pipeline transportation and pipeline facilities against cybersecurity threats, an act of terrorism, and other nefarious acts that jeopardize the physical security or cybersecurity of such transportation or facilities, consistent with the National Institute of Standards and Technology Framework for Improvement of Critical Infrastructure Cybersecurity and any update to such guidelines pursuant to section 2(c)(15) of the National Institute for Standards and Technology Act (15 U.S.C. 272(c)(15)).

(2) Updating such guidelines as necessary based on intelligence and risk assessments, but not less frequently than every three years, unless such guidelines are superseded by directives or regulations.

(3) Sharing of such guidelines and, as appropriate, intelligence and information regarding such security threats to pipeline transportation and pipeline facilities, as appropriate, with relevant Federal, State, local, Tribal, and territorial entities and public and private sector stakeholders.

(4) Conducting voluntary security assessments based on such guidelines, or mandatory security assessments if required by superseding directives or regulations, to provide recommendations or requirements for the improvement of the security of pipeline transportation and pipeline facilities against cybersecurity threats, an act of terrorism, and other nefarious acts that jeopardize the physical security or cybersecurity of such transpor-

tation or facilities, including the security policies, plans, practices, and training programs maintained by owners and operators of pipeline facilities.

(5) Carrying out a program through which the Administrator identifies and ranks the relative risk of pipelines and inspects pipeline facilities designated by owners and operators of such facilities as critical based on such guidelines or superseding directives or regulations.

(6) Supporting the development and implementation of a security directive or regulation when the Administrator issues such a directive or regulation.

(e) DETAILS.—In furtherance of the division's mission, as set forth in subsection (b), the Administrator and the Director of the Cybersecurity and Infrastructure Security Agency may detail personnel between their components to leverage expertise. Personnel detailed from the Cybersecurity and Infrastructure Security Agency may be considered as fulfilling the cybersecurity expertise requirements in referred to in subsection (c).

* * * * * * *

○