In this section, the word ''passenger'' is substituted for ''person'' for consistency in the revised title.

In subsection (a)(1), the words ''of his person'' are omitted as surplus.

In subsection (a)(2), the words ''or inspection'' are omitted as surplus.

In subsection (b), the words ''reasonable'' and ''also'' are omitted as surplus. The word ''rules'' is omitted as being synonymous with ''regulations''. The words ''the carrier decides is'' are substituted for ''when, in the opinion of the carrier, such transportation would'' to eliminate unnecessary words. The words ''of flight'' are omitted as surplus.

In subsection (c), the words ''for compensation or hire'' are omitted because of the definitions of ''air transportation'' and ''intrastate air transportation'' in section 40102(a) of the revised title. The word ''inspect'' is omitted as surplus.

AMENDMENTS

2018—Subsec. (a). Pub. L. 115–254, §1991(d)(2)(A), substituted ''Administrator of the Transportation Security Administration'' for ''Under Secretary of Transportation for Security'' in introductory provisions.

Subsec. (b). Pub. L. 115–254, §1991(d)(2)(B), substituted ''Administrator of the Transportation Security Administration'' for ''Under Secretary''.

2001—Subsec. (a). Pub. L. 107–71 substituted ''Under Secretary of Transportation for Security'' for ''Administrator of the Federal Aviation Administration'' in introductory provisions.

Subsec. (b). Pub. L. 107–71, §101(f)(7), substituted ''Under Secretary'' for ''Administrator''.

§ 44903. Air transportation security

(a) DEFINITIONS.—In this section:

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

(2) LAW ENFORCEMENT PERSONNEL.—The term ''law enforcement personnel'' means individuals—

(A) authorized to carry and use firearms;

(B) vested with the degree of the police power of arrest the Administrator considers necessary to carry out this section; and

(C) identifiable by appropriate indicia of authority.

(b) PROTECTION AGAINST VIOLENCE AND PIRACY.—The Administrator shall prescribe regulations to protect passengers and property on an aircraft operating in air transportation or intrastate air transportation against an act of criminal violence or aircraft piracy. When prescribing a regulation under this subsection, the Administrator shall—

(1) consult with the Secretary of Transportation, the Attorney General, the heads of other departments, agencies, and instrumentalities of the United States Government, and State and local authorities;

(2) consider whether a proposed regulation is consistent with—

(A) protecting passengers; and

(B) the public interest in promoting air transportation and intrastate air transportation;

(3) to the maximum extent practicable, require a uniform procedure for searching and detaining passengers and property to ensure—

(A) their safety; and

(B) courteous and efficient treatment by an air carrier, an agent or employee of an air carrier, and Government, State, and local law enforcement personnel carrying out this section; and

(4) consider the extent to which a proposed regulation will carry out this section.

(c) SECURITY PROGRAMS.—(1) The Administrator shall prescribe regulations under subsection (b) of this section that require each operator of an airport regularly serving an air carrier holding a certificate issued by the Secretary of Transportation to establish an air transportation security program that provides a law enforcement presence and capability at each of those airports that is adequate to ensure the safety of passengers. The regulations shall authorize the operator to use the services of qualified State, local, and private law enforcement personnel. When the Administrator decides, after being notified by an operator in the form the Administrator prescribes, that not enough qualified State, local, and private law enforcement personnel are available to carry out subsection (b), the Administrator may authorize the operator to use, on a reimbursable basis, personnel employed by the Administrator, or by another department, agency, or instrumentality of the Government with the consent of the head of the department, agency, or instrumentality, to supplement State, local, and private law enforcement personnel. When deciding whether additional personnel are needed, the Administrator shall consider the number of passengers boarded at the airport, the extent of anticipated risk of criminal violence or aircraft piracy at the airport or to the air carrier aircraft operations at the airport, and the availability of qualified State or local law enforcement personnel at the airport.

(2)(A) The Administrator may approve a security program of an airport operator, or an amendment in an existing program, that incorporates a security program of an airport tenant (except an air carrier separately complying with part 108 or 129 of title 14, Code of Federal Regulations) having access to a secured area of the airport, if the program or amendment incorporates—

(i) the measures the tenant will use, within the tenant's leased areas or areas designated for the tenant's exclusive use under an agreement with the airport operator, to carry out the security requirements imposed by the Administrator on the airport operator under the access control system requirements of section 107.14 of title 14, Code of Federal Regulations, or under other requirements of part 107 of title 14; and

(ii) the methods the airport operator will use to monitor and audit the tenant's compliance with the security requirements and provides that the tenant will be required to pay monetary penalties to the airport operator if the tenant fails to carry out a security requirement under a contractual provision or requirement imposed by the airport operator.

(B) If the Administrator approves a program or amendment described in subparagraph (A) of this paragraph, the airport operator may not be found to be in violation of a requirement of this subsection or subsection (b) of this section when

the airport operator demonstrates that the tenant or an employee, permittee, or invitee of the tenant is responsible for the violation and that the airport operator has complied with all measures in its security program for securing compliance with its security program by the tenant.

(C) MAXIMUM USE OF CHEMICAL AND BIOLOGICAL WEAPON DETECTION EQUIPMENT.—The Secretary of Transportation may require airports to maximize the use of technology and equipment that is designed to detect or neutralize potential chemical or biological weapons.

(3) PILOT PROGRAMS.—The Administrator shall establish pilot programs in no fewer than 20 airports to test and evaluate new and emerging technology for providing access control and other security protections for closed or secure areas of the airports. Such technology may include biometric or other technology that ensures only authorized access to secure areas.

(d) AUTHORIZING INDIVIDUALS TO CARRY FIREARMS AND MAKE ARRESTS.—With the approval of the Attorney General and the Secretary of State, the Administrator may authorize an individual who carries out air transportation security duties—

(1) to carry firearms; and

(2) to make arrests without warrant for an offense against the United States committed in the presence of the individual or for a felony under the laws of the United States, if the individual reasonably believes the individual to be arrested has committed or is committing a felony.

(e) EXCLUSIVE RESPONSIBILITY OVER PASSENGER SAFETY.—The Administrator has the exclusive responsibility to direct law enforcement activity related to the safety of passengers on an aircraft involved in an offense under section 46502 of this title from the moment all external doors of the aircraft are closed following boarding until those doors are opened to allow passengers to leave the aircraft. When requested by the Administrator, other departments, agencies, and instrumentalities of the Government shall provide assistance necessary to carry out this subsection.

(f) GOVERNMENT AND INDUSTRY CONSORTIA.—The Administrator may establish at airports such consortia of government and aviation industry representatives as the Administrator may designate to provide advice on matters related to aviation security and safety. Such consortia shall not be considered Federal advisory committees for purposes of the Federal Advisory Committee Act (5 U.S.C. App.).

(g) IMPROVEMENT OF SECURED-AREA ACCESS CONTROL.—

(1) ENFORCEMENT.—

(A) ADMINISTRATOR TO PUBLISH SANCTIONS.—The Administrator shall publish in the Federal Register a list of sanctions for use as guidelines in the discipline of employees for infractions of airport access control requirements. The guidelines shall incorporate a progressive disciplinary approach that relates proposed sanctions to the severity or recurring nature of the infraction and shall include measures such as remedial training, suspension from security-related duties, suspension from all duties without pay, and termination of employment.

(B) USE OF SANCTIONS.—Each airport operator, air carrier, and security screening company shall include the list of sanctions published by the Administrator in its security program. The security program shall include a process for taking prompt disciplinary action against an employee who commits an infraction of airport access control requirements.

(2) IMPROVEMENTS.—The Administrator shall—

(A) work with airport operators and air carriers to implement and strengthen existing controls to eliminate airport access control weaknesses;

(B) require airport operators and air carriers to develop and implement comprehensive and recurring training programs that teach employees their roles in airport security, the importance of their participation, how their performance will be evaluated, and what action will be taken if they fail to perform;

(C) require airport operators and air carriers to develop and implement programs that foster and reward compliance with airport access control requirements and discourage and penalize noncompliance in accordance with guidelines issued by the Administrator to measure employee compliance;

(D) on an ongoing basis, assess and test for compliance with access control requirements, report annually findings of the assessments, and assess the effectiveness of penalties in ensuring compliance with security procedures and take any other appropriate enforcement actions when noncompliance is found;

(E) improve and better administer the Administrator's security database to ensure its efficiency, reliability, and usefulness for identification of systemic problems and allocation of resources;

(F) improve the execution of the Administrator's quality control program; and

(G) work with airport operators to strengthen access control points in secured areas (including air traffic control operations areas, maintenance areas, crew lounges, baggage handling areas, concessions, and catering delivery areas) to ensure the security of passengers and aircraft and consider the deployment of biometric or similar technologies that identify individuals based on unique personal characteristics.

(h) IMPROVED AIRPORT PERIMETER ACCESS SECURITY.—

(1) IN GENERAL.—The Administrator, in consultation with the airport operator and law enforcement authorities, may order the deployment of such personnel at any secure area of the airport as necessary to counter the risk of criminal violence, the risk of aircraft piracy at the airport, the risk to air carrier aircraft operations at the airport, or to meet national security concerns.

(2) SECURITY OF AIRCRAFT AND GROUND ACCESS TO SECURE AREAS.—In determining where to

deploy such personnel, the Administrator shall consider the physical security needs of air traffic control facilities, parked aircraft, aircraft servicing equipment, aircraft supplies (including fuel), automobile parking facilities within airport perimeters or adjacent to secured facilities, and access and transition areas at airports served by other means of ground or water transportation.

(3) DEPLOYMENT OF FEDERAL LAW ENFORCEMENT PERSONNEL.—The Secretary of Homeland Security may enter into a memorandum of understanding or other agreement with the Attorney General or the head of any other appropriate Federal law enforcement agency to deploy Federal law enforcement personnel at an airport in order to meet aviation safety and security concerns.

(4) AIRPORT PERIMETER SCREENING.—The Administrator—

(A) shall require screening or inspection of all individuals, goods, property, vehicles, and other equipment before entry into a secured area of an airport in the United States described in section 44903(c);[1]

(B) shall prescribe specific requirements for such screening and inspection that will assure at least the same level of protection as will result from screening of passengers and their baggage;

(C) shall establish procedures to ensure the safety and integrity of—

(i) all persons providing services with respect to aircraft providing passenger air transportation or intrastate air transportation and facilities of such persons at an airport in the United States described in subsection (c);

(ii) all supplies, including catering and passenger amenities, placed aboard such aircraft, including the sealing of supplies to ensure easy visual detection of tampering; and

(iii) all persons providing such supplies and facilities of such persons;

(D) shall require vendors having direct access to the airfield and aircraft to develop security programs; and

(E) shall issue guidance for the use of biometric or other technology that positively verifies the identity of each employee and law enforcement officer who enters a secure area of an airport.

(5) USE OF BIOMETRIC TECHNOLOGY IN AIRPORT ACCESS CONTROL SYSTEMS.—In issuing guidance under paragraph (4)(E), the Administrator in consultation with representatives of the aviation industry, the biometric identifier industry, and the National Institute of Standards and Technology, shall establish, at a minimum—

(A) comprehensive technical and operational system requirements and performance standards for the use of biometric identifier technology in airport access control systems (including airport perimeter access control systems) to ensure that the biometric identifier systems are effective, reliable, and secure;

(B) a list of products and vendors that meet the requirements and standards set forth in subparagraph (A);

(C) procedures for implementing biometric identifier systems—

(i) to ensure that individuals do not use an assumed identity to enroll in a biometric identifier system; and

(ii) to resolve failures to enroll, false matches, and false non-matches; and

(D) best practices for incorporating biometric identifier technology into airport access control systems in the most effective manner, including a process to best utilize existing airport access control systems, facilities, and equipment and existing data networks connecting airports.

(6) USE OF BIOMETRIC TECHNOLOGY FOR ARMED LAW ENFORCEMENT TRAVEL.—

(A) IN GENERAL.—The Secretary of Homeland Security, in consultation with the Attorney General, shall—

(i) implement this paragraph by publication in the Federal Register; and

(ii) establish a national registered armed law enforcement program, that shall be federally managed, for law enforcement officers needing to be armed when traveling by commercial aircraft.

(B) PROGRAM REQUIREMENTS.—The program shall—

(i) establish a credential or a system that incorporates biometric technology and other applicable technologies;

(ii) establish a system for law enforcement officers who need to be armed when traveling by commercial aircraft on a regular basis and for those who need to be armed during temporary travel assignments;

(iii) comply with other uniform credentialing initiatives, including the Homeland Security Presidential Directive 12;

(iv) apply to all Federal, State, local, tribal, and territorial government law enforcement agencies; and

(v) establish a process by which the travel credential or system may be used to verify the identity, using biometric technology, of a Federal, State, local, tribal, or territorial law enforcement officer seeking to carry a weapon on board a commercial aircraft, without unnecessarily disclosing to the public that the individual is a law enforcement officer.

(C) PROCEDURES.—In establishing the program, the Secretary of Homeland Security shall develop procedures—

(i) to ensure that a law enforcement officer of a Federal, State, local, tribal, or territorial government flying armed has a specific reason for flying armed and the reason is within the scope of the duties of such officer;

(ii) to preserve the anonymity of the armed law enforcement officer;

(iii) to resolve failures to enroll, false matches, and false nonmatches relating to the use of the law enforcement travel credential or system;

[1] So in original. Probably should be ''subsection (c)''.

(iv) to determine the method of issuance of the biometric credential to law enforcement officers needing to be armed when traveling by commercial aircraft;

(v) to invalidate any law enforcement travel credential or system that is lost, stolen, or no longer authorized for use;

(vi) to coordinate the program with the Federal Air Marshal Service, including the force multiplier program of the Service; and

(vii) to implement a phased approach to launching the program, addressing the immediate needs of the relevant Federal agent population before expanding to other law enforcement populations.

(7) DEFINITIONS.—In this subsection, the following definitions apply:

(A) BIOMETRIC IDENTIFIER INFORMATION.—The term ''biometric identifier information'' means the distinct physical or behavioral characteristics of an individual that are used for unique identification, or verification of the identity, of an individual.

(B) BIOMETRIC IDENTIFIER.—The term ''biometric identifier'' means a technology that enables the automated identification, or verification of the identity, of an individual based on biometric information.

(C) FAILURE TO ENROLL.—The term ''failure to enroll'' means the inability of an individual to enroll in a biometric identifier system due to an insufficiently distinctive biometric sample, the lack of a body part necessary to provide the biometric sample, a system design that makes it difficult to provide consistent biometric identifier information, or other factors.

(D) FALSE MATCH.—The term ''false match'' means the incorrect matching of one individual's biometric identifier information to another individual's biometric identifier information by a biometric identifier system.

(E) FALSE NON-MATCH.—The term ''false non-match'' means the rejection of a valid identity by a biometric identifier system.

(F) SECURE AREA OF AN AIRPORT.—The term ''secure area of an airport'' means the sterile area and the Secure Identification Display Area of an airport (as such terms are defined in section 1540.5 of title 49, Code of Federal Regulations, or any successor regulation to such section).

(i) AUTHORITY TO ARM FLIGHT DECK CREW WITH LESS-THAN-LETHAL WEAPONS.—

(1) IN GENERAL.—If the Administrator, after receiving the recommendations of the National Institute of Justice, determines, with the approval of the Attorney General and the Secretary of State, that it is appropriate and necessary and would effectively serve the public interest in avoiding air piracy, the Administrator may authorize members of the flight deck crew on any aircraft providing air transportation or intrastate air transportation to carry a less-than-lethal weapon while the aircraft is engaged in providing such transportation.

(2) USAGE.—If the Administrator grants authority under paragraph (1) for flight deck crew members to carry a less-than-lethal weapon while engaged in providing air transportation or intrastate air transportation, the Administrator shall—

(A) prescribe rules requiring that any such crew member be trained in the proper use of the weapon; and

(B) prescribe guidelines setting forth the circumstances under which such weapons may be used.

(3) REQUEST OF AIR CARRIERS TO USE LESS-THAN-LETHAL WEAPONS.—If the Administrator receives a request from an air carrier for authorization to allow pilots of the air carrier to carry less-than-lethal weapons, the Administrator shall respond to that request within 90 days.

(j) SHORT-TERM ASSESSMENT AND DEPLOYMENT OF EMERGING SECURITY TECHNOLOGIES AND PROCEDURES.—

(1) IN GENERAL.—The Administrator shall periodically recommend to airport operators commercially available measures or procedures to prevent access to secure airport areas by unauthorized persons.

(2) SECURE FLIGHT PROGRAM.—

(A) IN GENERAL.—The Administrator shall ensure that the Secure Flight program, or any successor program—

(i) is used to evaluate all passengers before they board an aircraft; and

(ii) includes procedures to ensure that individuals selected by the program and their carry-on and checked baggage are adequately screened.

(B) MODIFICATIONS.—The Administrator may modify any requirement under the Secure Flight program for flights that originate and terminate within the same State, if the Administrator determines that—

(i) the State has extraordinary air transportation needs or concerns due to its isolation and dependence on air transportation; and

(ii) the routine characteristics of passengers, given the nature of the market, regularly triggers primary selectee status.

(C) ADVANCED AIRLINE PASSENGER PRESCREENING.—

(i) COMMENCEMENT OF TESTING.—The Administrator shall commence testing of an advanced passenger prescreening system that will allow the Department of Homeland Security to assume the performance of comparing passenger information, as defined by the Administrator, to the automatic selectee and no fly lists, utilizing all appropriate records in the consolidated and integrated terrorist watchlist maintained by the Federal Government.

(ii) ASSUMPTION OF FUNCTION.—The Administrator, or the designee of the Administrator, shall begin to assume the performance of the passenger prescreening function of comparing passenger information to the automatic selectee and no fly lists and utilize all appropriate records in the consolidated and integrated terrorist watchlist maintained by the Federal Government in performing that function.

(iii) REQUIREMENTS.—In assuming performance of the function under clause (ii), the Administrator shall—

(I) establish a procedure to enable airline passengers, who are delayed or prohibited from boarding a flight because the advanced passenger prescreening system determined that they might pose a security threat, to appeal such determination and correct information contained in the system;

(II) ensure that Federal Government databases that will be used to establish the identity of a passenger under the system will not produce a large number of false positives;

(III) establish an internal oversight board to oversee and monitor the manner in which the system is being implemented;

(IV) establish sufficient operational safeguards to reduce the opportunities for abuse;

(V) implement substantial security measures to protect the system from unauthorized access;

(VI) adopt policies establishing effective oversight of the use and operation of the system; and

(VII) ensure that there are no specific privacy concerns with the technological architecture of the system.

(iv) PASSENGER INFORMATION.—After the completion of the testing of the advanced passenger prescreening system, the Administrator, by order or interim final rule—

(I) shall require air carriers to supply to the Administrator the passenger information needed to begin implementing the advanced passenger prescreening system; and

(II) shall require entities that provide systems and services to air carriers in the operation of air carrier reservations systems to provide to air carriers passenger information in possession of such entities, but only to the extent necessary to comply with subclause (I).

(v) INCLUSION OF DETAINEES ON NO FLY LIST.—The Administrator, in coordination with the Terrorist Screening Center, shall include on the No Fly List any individual who was a detainee held at the Naval Station, Guantanamo Bay, Cuba, unless the President certifies in writing to Congress that the detainee poses no threat to the United States, its citizens, or its allies. For purposes of this clause, the term ''detainee'' means an individual in the custody or under the physical control of the United States as a result of armed conflict.

(D) SCREENING OF EMPLOYEES AGAINST WATCHLIST.—The Administrator, in coordination with the Secretary of Transportation and the Administrator of the Federal Aviation Administration, shall ensure that individuals are screened against all appropriate records in the consolidated and integrated terrorist watchlist maintained by the Federal Government before—

(i) being certificated by the Federal Aviation Administration;

(ii) being granted unescorted access to the secure area of an airport; or

(iii) being granted unescorted access to the air operations area (as defined in section 1540.5 of title 49, Code of Federal Regulations, or any successor regulation to such section) of an airport.

(E) AIRCRAFT CHARTER CUSTOMER AND LESSEE PRESCREENING.—

(i) IN GENERAL.—The Administrator Administrator[2] shall establish a process by which operators of aircraft to be used in charter air transportation with a maximum takeoff weight greater than 12,500 pounds and lessors of aircraft with a maximum takeoff weight greater than 12,500 pounds may—

(I) request the Department of Homeland Security to use the advanced passenger prescreening system to compare information about any individual seeking to charter an aircraft with a maximum takeoff weight greater than 12,500 pounds, any passenger proposed to be transported aboard such aircraft, and any individual seeking to lease an aircraft with a maximum takeoff weight greater than 12,500 pounds to the automatic selectee and no fly lists, utilizing all appropriate records in the consolidated and integrated terrorist watchlist maintained by the Federal Government; and

(II) refuse to charter or lease an aircraft with a maximum takeoff weight greater than 12,500 pounds to or transport aboard such aircraft any persons identified on such watch list.

(ii) REQUIREMENTS.—The requirements of subparagraph (C)(iii) shall apply to this subparagraph.

(iii) NO FLY AND AUTOMATIC SELECTEE LISTS.—The Secretary of Homeland Security, in consultation with the Terrorist Screening Center, shall design and review, as necessary, guidelines, policies, and operating procedures for the collection, removal, and updating of data maintained, or to be maintained, in the no fly and automatic selectee lists.

(F) APPLICABILITY.—Section 607 of the Vision 100—Century of Aviation Reauthorization Act (49 U.S.C. 44903 note; 117 Stat. 2568) shall not apply to the advanced passenger prescreening system established under subparagraph (C).

(G) APPEAL PROCEDURES.—

(i) IN GENERAL.—The Administrator shall establish a timely and fair process for individuals identified as a threat under one or more of subparagraphs (C), (D), and (E) to appeal to the Transportation Security Administration the determination and correct any erroneous information.

[2] So in original.

(ii) RECORDS.—The process shall include the establishment of a method by which the Administrator will be able to maintain a record of air passengers and other individuals who have been misidentified and have corrected erroneous information. To prevent repeated delays of misidentified passengers and other individuals, the Transportation Security Administration record shall contain information determined by the Administrator to authenticate the identity of such a passenger or individual.

(H) DEFINITION.—In this paragraph, the term ''secure area of an airport'' means the sterile area and the Secure Identification Display Area of an airport (as such terms are defined in section 1540.5 of title 49, Code of Federal Regulations, or any successor regulation to such section).

(k) LIMITATION ON LIABILITY FOR ACTS TO THWART CRIMINAL VIOLENCE OR AIRCRAFT PIRACY.—An individual shall not be liable for damages in any action brought in a Federal or State court arising out of the acts of the individual in attempting to thwart an act of criminal violence or piracy on an aircraft if that individual reasonably believed that such an act of criminal violence or piracy was occurring or was about to occur.

(*l*) AIR CHARTER PROGRAM.—

(1) IN GENERAL.—The Administrator shall implement an aviation security program for charter air carriers (as defined in section 40102(a)) with a maximum certificated takeoff weight of more than 12,500 pounds.

(2) EXEMPTION FOR ARMED FORCES CHARTERS.—

(A) IN GENERAL.—Paragraph (1) and the other requirements of this chapter do not apply to passengers and property carried by aircraft when employed to provide charter transportation to members of the armed forces.

(B) SECURITY PROCEDURES.—The Secretary of Defense, in consultation with the Secretary of Homeland Security and the Secretary of Transportation, shall establish security procedures relating to the operation of aircraft when employed to provide charter transportation to members of the armed forces to or from an airport described in section 44903(c).

(C) ARMED FORCES DEFINED.—In this paragraph, the term ''armed forces'' has the meaning given that term by section 101(a)(4) of title 10.

(m) SECURITY SCREENING FOR MEMBERS OF THE ARMED FORCES.—

(1) IN GENERAL.—The Administrator, in consultation with the Department of Defense, shall develop and implement a plan to provide expedited security screening services for a member of the armed forces, and, to the extent possible, any accompanying family member, if the member of the armed forces, while in uniform, presents documentation indicating official orders for air transportation departing from a primary airport (as defined in section 47102).

(2) PROTOCOLS.—In developing the plan, the Administrator shall consider—

(A) leveraging existing security screening models used to reduce passenger wait times;

(B) establishing standard guidelines for the screening of military uniform items, including combat boots; and

(C) incorporating any new screening protocols into an existing trusted passenger program, as established pursuant to section 109(a)(3) of the Aviation and Transportation Security Act (49 U.S.C. 114 note), or into the development of any new credential or system that incorporates biometric technology and other applicable technologies to verify the identity of individuals traveling in air transportation.

(3) RULE OF CONSTRUCTION.—Nothing in this subsection shall affect the authority of the Administrator to require additional screening of a member of the armed forces if intelligence or law enforcement information indicates that additional screening is necessary.

(4) REPORT TO CONGRESS.—The Administrator shall submit to the appropriate committees of Congress a report on the implementation of the plan.

(n) PASSENGER EXIT POINTS FROM STERILE AREA.—

(1) IN GENERAL.—The Secretary of Homeland Security shall ensure that the Transportation Security Administration is responsible for monitoring passenger exit points from the sterile area of airports at which the Transportation Security Administration provided such monitoring as of December 1, 2013.

(2) STERILE AREA DEFINED.—In this section, the term ''sterile area'' has the meaning given that term in section 1540.5 of title 49, Code of Federal Regulations (or any corresponding similar regulation or ruling).

(Pub. L. 103–272, § 1(e), July 5, 1994, 108 Stat. 1205; Pub. L. 106–181, title VII, § 717, Apr. 5, 2000, 114 Stat. 163; Pub. L. 106–528, §§ 4, 6, Nov. 22, 2000, 114 Stat. 2520, 2521; Pub. L. 107–71, title I, §§ 101(f)(7)–(9), 106(a), (c), (d), 120, 126(b), 136, 144, Nov. 19, 2001, 115 Stat. 603, 608–610, 629, 632, 636, 644; Pub. L. 107–296, title XIV, §§ 1405, 1406, Nov. 25, 2002, 116 Stat. 2307; Pub. L. 108–176, title VI, § 606(a), Dec. 12, 2003, 117 Stat. 2568; Pub. L. 108–458, title IV, §§ 4011(a), 4012(a)(1), Dec. 17, 2004, 118 Stat. 3712, 3714; Pub. L. 110–53, title XVI, § 1615(a), Aug. 3, 2007, 121 Stat. 486; Pub. L. 111–83, title V, § 553, Oct. 28, 2009, 123 Stat. 2179; Pub. L. 112–86, § 2(a), Jan. 3, 2012, 125 Stat. 1874; Pub. L. 113–67, div. A, title VI, § 603, Dec. 26, 2013, 127 Stat. 1188; Pub. L. 115–254, div. K, title I, § 1991(d)(3), Oct. 5, 2018, 132 Stat. 3630.)

HISTORICAL AND REVISION NOTES

Revised Section	*Source (U.S. Code)*	*Source (Statutes at Large)*
44903(a)	49 App.:1357(f).	Aug. 23, 1958, Pub. L. 85–726, 72 Stat. 731, § 316(a), (b), (e)(2), (3), (f); added Aug. 5, 1974, Pub. L. 93–366, § 202, 88 Stat. 415, 417.
44903(b)	49 App.:1357(a).	
44903(c)(1) ..	49 App.:1357(b).	
44903(c)(2) ..	49 App.:1357(g).	Aug. 23, 1958, Pub. L. 85–726, 72 Stat. 731, § 316(g); added Aug. 15, 1990, Pub. L. 101–370, § 2, 104 Stat. 451.

HISTORICAL AND REVISION NOTES—CONTINUED

Revised Section	*Source (U.S. Code)*	*Source (Statutes at Large)*
44903(d)	49 App.:1356b.	Aug. 8, 1985, Pub. L. 99–83, § 553(b), 99 Stat. 226.
44903(e)	49 App.:1357(e)(2), (3).	

In this section, the word ''passengers'' is substituted for ''persons'' for consistency in the revised title.

In subsection (a)(2), the words ''the degree of'' are substituted for ''such'' for clarity.

In subsection (b), before clause (1), the word ''rules'' is omitted as being synonymous with ''regulations''. The words ''such reasonable . . . requiring such practices, methods, and procedures, or governing the design, materials, and construction of aircraft, as he may deem necessary'' are omitted as surplus. The word ''air'' after ''intrastate'' is added for clarity and consistency. The words ''and amending'' are omitted as surplus. In clause (1), the words ''the heads of other departments, agencies, and instrumentalities of the United States Government, and State and local authorities'' are substituted for ''such other Federal, State, and local agencies'' for consistency in the revised title and with other titles of the United States Code. The words ''as he may deem appropriate'' are omitted as surplus. In clause (2)(A), the words ''in air transportation or intrastate air transportation against acts of criminal violence and aircraft piracy'' are omitted as surplus. In clause (3), before subclause (A), the words ''inspection'' and ''in air transportation and intrastate air transportation'' are omitted as surplus. In subclause (B), the words ''that they will receive'' and ''any air transportation security program established under'' are omitted as surplus. In clause (4), the words ''contribute to . . . the purposes of'' are omitted as surplus.

In subsection (c)(1), the words ''traveling in air transportation or intrastate air transportation from acts of criminal violence and aircraft piracy'' and ''whose services are made available by their employers'' are omitted as surplus. The words ''department, agency, or instrumentality of the Government'' are substituted for ''Federal department or agency'' for consistency in the revised title and with other titles of the Code. The word ''When'' is substituted for ''In any case in which'' to eliminate unnecessary words. The words ''receipt of'', ''by order'', ''the services of'', ''directly'', and ''at the airport concerned in such numbers and for such period of time as the Administrator may deem necessary'' are omitted as surplus. The words ''When deciding whether additional personnel are needed'' are substituted for ''In making the determination referred to in the preceding sentence'' for clarity.

In subsection (c)(2)(A), before clause (i), the words ''under this section'' are omitted as surplus. The words ''or an amendment in an existing program'' are substituted for ''and may approve an amendment to a security program of an airport operator approved by the Administrator under subsection (b)'' to eliminate unnecessary words. In clause (ii), the word ''monetary'' is substituted for ''financial'' for consistency.

In subsection (e), the words ''Notwithstanding any other provisions of law'', ''the commission of'', ''considered'', and ''the moment when'' before ''such door'' are omitted as surplus. The words ''to allow passengers to leave'' are substituted for ''disembarkation'', and the words ''the aircraft'' are added, for clarity. The words ''departments, agencies, and instrumentalities of the Government'' are substituted for ''Federal departments and agencies'' for consistency in the revised title and with other titles of the Code. The words ''as may be . . . the purposes of'' are omitted as surplus.

REFERENCES IN TEXT

The Federal Advisory Committee Act, referred to in subsec. (f), is Pub. L. 92–463, Oct. 6, 1972, 86 Stat. 770, as amended, which is set out in the Appendix to Title 5, Government Organization and Employees.

Section 607 of the Vision 100—Century of Aviation Reauthorization Act, referred to in subsec. (j)(2)(F), is section 607 of Pub. L. 108–176, which is set out as a note below.

AMENDMENTS

2018—Pub. L. 115–254, § 1991(d)(3)(I), substituted ''Administrator'' for ''Under Secretary'' wherever appearing.

Subsec. (a). Pub. L. 115–254, § 1991(d)(3)(A), substituted ''Definitions'' for ''Definition'' in heading and ''In this section:'' for ''In this section, 'law enforcement personnel' means individuals—'' in introductory provisions, added par. (1), redesignated former pars. (1) to (3) as subpars. (A) to (C) of par. (2), inserted before subpar. (A) ''(2) LAW ENFORCEMENT PERSONNEL.—The term 'law enforcement personnel' means individuals—'', and in subpar. (B) substituted ''Administrator'' for ''Under Secretary of Transportation for Security''.

Subsec. (d). Pub. L. 115–254, § 1991(d)(3)(B), substituted ''Administrator'' for ''Secretary of Transportation'' in introductory provisions.

Subsec. (g)(2)(E), (F). Pub. L. 115–254, § 1991(d)(3)(C), substituted ''Administrator's'' for ''Under Secretary's''.

Subsec. (h)(3). Pub. L. 115–254, § 1991(d)(3)(D)(i), substituted ''Secretary of Homeland Security'' for ''Secretary''.

Subsec. (h)(4)(A). Pub. L. 115–254, § 1991(d)(3)(D)(ii)(I), struck out '', as soon as practicable after the date of enactment of this subsection,'' after ''shall require''.

Subsec. (h)(4)(C)(i). Pub. L. 115–254, § 1991(d)(3)(D)(ii)(II), substituted ''subsection (c)'' for ''section 44903(c)''.

Subsec. (h)(4)(E). Pub. L. 115–254, § 1991(d)(3)(D)(ii)(III), struck out '', not later than March 31, 2005,'' after ''shall issue''.

Subsec. (h)(5). Pub. L. 115–254, § 1991(d)(3)(D)(iii), substituted ''Administrator'' for ''Assistant Secretary of Homeland Security (Transportation Security Administration)'' in introductory provisions.

Subsec. (h)(6)(A). Pub. L. 115–254, § 1991(d)(3)(D)(iv)(I), substituted ''The'' for ''Not later than 18 months after the date of enactment of the Implementing Recommendations of the 9/11 Commission Act of 2007, the'' in introductory provisions.

Subsec. (h)(6)(A)(i). Pub. L. 115–254, § 1991(d)(3)(D)(iv)(II), substituted ''paragraph'' for ''section''.

Subsec. (h)(6)(C). Pub. L. 115–254, § 1991(d)(3)(D)(v), substituted ''Secretary of Homeland Security'' for ''Secretary'' in introductory provisions.

Subsec. (i)(3). Pub. L. 115–254, § 1991(d)(3)(E), struck out '', after the date of enactment of this paragraph,'' after ''If''.

Subsec. (j)(1). Pub. L. 115–254, § 1991(d)(3)(F)(i), amended par. (1) generally. Prior to amendment, par. (1) required the Under Secretary of Transportation for Security to recommend to airport operators, within 6 months after Nov. 19, 2001, commercially available measures or procedures to prevent access to secure airport areas by unauthorized persons.

Subsec. (j)(2). Pub. L. 115–254, § 1991(d)(3)(F)(ii)(VII), substituted ''Administrator'' for ''Assistant Secretary'' wherever appearing.

Pub. L. 115–254, § 1991(d)(3)(F)(ii)(I), substituted ''Secure flight program'' for ''Computer-assisted passenger prescreening system'' in heading.

Subsec. (j)(2)(A). Pub. L. 115–254, § 1991(d)(3)(F)(ii)(II), substituted ''Administrator'' for ''Secretary of Transportation'', ''Secure Flight program'' for ''Computer-Assisted Passenger Prescreening System'', and, in two places, ''program'' for ''system''.

Subsec. (j)(2)(B). Pub. L. 115–254, § 1991(d)(3)(F)(ii)(III), in introductory provisions, substituted ''Administrator'' for ''Secretary of Transportation'', ''Secure Flight program'' for ''Computer-Assisted Passenger Prescreening System'', and ''Administrator'' for ''Secretary''.

Subsec. (j)(2)(C)(i). Pub. L. 115–254, § 1991(d)(3)(F)(ii)(IV)(aa), substituted ''The Adminis-

trator'' for ''Not later than January 1, 2005, the Assistant Secretary of Homeland Security (Transportation Security Administration), or the designee of the Assistant Secretary,''.

Subsec. (j)(2)(C)(ii). Pub. L. 115–254, §1991(d)(3)(F)(ii)(IV)(bb), substituted ''The'' for ''Not later than 180 days after completion of testing under clause (i), the''.

Subsec. (j)(2)(C)(iv). Pub. L. 115–254, §1991(d)(3)(F)(ii)(IV)(cc), substituted ''After'' for ''Not later than 180 days after'' in introductory provisions.

Subsec. (j)(2)(D). Pub. L. 115–254, §1991(d)(3)(F)(ii)(V), substituted ''Administrator'' for ''Assistant Secretary of Homeland Security (Transportation Security Administration)'' in introductory provisions.

Subsec. (j)(2)(E)(i). Pub. L. 115–254, §1991(d)(3)(F)(ii)(VI), substituted ''The Administrator'' for ''Not later than 90 days after the date on which the Assistant Secretary assumes the performance of the advanced passenger prescreening function under subparagraph (C)(ii), the'' in introductory provisions.

Subsec. (*l*)(1). Pub. L. 115–254, §1991(d)(3)(G), substituted ''Administrator'' for ''Under Secretary for Border and Transportation Security of the Department of Homeland Security''.

Subsec. (m). Pub. L. 115–254, §1991(d)(3)(H)(ii), substituted ''Administrator'' for ''Assistant Secretary'' wherever appearing.

Subsec. (m)(1). Pub. L. 115–254, §1991(d)(3)(H)(i), substituted ''Administrator'' for ''Assistant Secretary of Homeland Security (Transportation Security Administration)''.

2013—Subsec. (n). Pub. L. 113–67 added subsec. (n).

2012—Subsec. (m). Pub. L. 112–86 added subsec. (m).

2009—Subsec. (j)(2)(C)(v). Pub. L. 111–83 added cl. (v).

2007—Subsec. (h)(6). Pub. L. 110–53 amended par. (6) generally. Prior to amendment, par. (6) related to establishment of a uniform law enforcement officer travel credential incorporating biometric identifier technology not later than 120 days after Dec. 17, 2004.

2004—Subsec. (h)(4)(E). Pub. L. 108–458, §4011(a)(1), substituted ''shall issue, not later than March 31, 2005, guidance for'' for ''may provide for''.

Subsec. (h)(5) to (7). Pub. L. 108–458, §4011(a)(2), added pars. (5) to (7).

Subsec. (j)(2)(C) to (H). Pub. L. 108–458, §4012(a)(1), added subpars. (C) to (H).

2003—Subsec. (*l*). Pub. L. 108–176 added subsec. (*l*).

2002—Subsec. (h). Pub. L. 107–296, §1406(3), redesignated subsec. (h), relating to limitation on liability for acts to thwart criminal violence or aircraft piracy, as (k).

Pub. L. 107–296, §1406(2), redesignated subsec. (h), relating to authority to arm flight deck crews with less-than-lethal weapons, as (i).

Subsec. (i). Pub. L. 107–296, §1406(2), redesignated subsec. (h), relating to authority to arm flight deck crews with less-than-lethal weapons, as (i). Former subsec. (i) redesignated (j).

Subsec. (i)(1). Pub. L. 107–296, §1405(b)(1), substituted ''If the Under Secretary'' for ''If the Secretary'' and ''the Under Secretary may'' for ''the Secretary may''.

Subsec. (i)(2). Pub. L. 107–296, §1405(b)(2), substituted ''Under Secretary'' for ''Secretary'' in two places in introductory provisions.

Subsec. (i)(3). Pub. L. 107–296, §1405(a), added par. (3).

Subsec. (j). Pub. L. 107–296, §1406(1), redesignated subsec. (i) as (j).

Subsec. (k). Pub. L. 107–296, §1406(3), redesignated subsec. (h), relating to limitation on liability for acts to thwart criminal violence or aircraft piracy, as (k).

2001—Subsec. (a)(2). Pub. L. 107–71, §101(f)(7), (9), substituted ''Under Secretary of Transportation for Security'' for ''Administrator of the Federal Aviation Administration''.

Subsec. (b). Pub. L. 107–71, §101(f)(7), substituted ''Under Secretary'' for ''Administrator'' in two places in introductory provisions.

Subsec. (c)(1), (2)(A), (B). Pub. L. 107–71, §101(f)(7), substituted ''Under Secretary'' for ''Administrator'' wherever appearing.

Subsec. (c)(2)(C). Pub. L. 107–71, §120, amended heading and text of subpar. (C) generally, substituting provisions relating to maximum use of chemical and biological weapon detection equipment for provisions relating to a manual process at explosive detection locations for randomly selecting additional checked bags for screening.

Subsec. (c)(3). Pub. L. 107–71, §106(d), added par. (3).

Subsecs. (e), (f), (g)(1)(A), (B). Pub. L. 107–71, §101(f)(7), substituted ''Under Secretary'' for ''Administrator'' wherever appearing.

Subsec. (g)(2). Pub. L. 107–71, §101(f)(7), substituted ''Under Secretary'' for ''Administrator'' in introductory provisions.

Subsec. (g)(2)(A). Pub. L. 107–71, §106(c)(1), substituted ''weaknesses;'' for ''weaknesses by January 31, 2001;''.

Subsec. (g)(2)(D). Pub. L. 107–71, §106(c)(2), added subpar. (D) and struck out former subpar. (D) which read as follows: ''assess and test for compliance with access control requirements, report findings, and assess penalties or take other appropriate enforcement actions when noncompliance is found;''.

Subsec. (g)(2)(C). Pub. L. 107–71, §101(f)(7), substituted ''Under Secretary'' for ''Administrator''.

Subsec. (g)(2)(E). Pub. L. 107–71, §101(f)(8), substituted ''Under Secretary's'' for ''Administrator's''.

Subsec. (g)(2)(F). Pub. L. 107–71, §§101(f)(8), 106(c)(3), substituted ''Under Secretary's'' for ''Administrator's'' and ''program;'' for ''program by January 31, 2001;''.

Subsec. (g)(2)(G). Pub. L. 107–71, §106(c)(4), added subpar. (G) and struck out former subpar. (G) which read as follows: ''require airport operators and air carriers to strengthen access control points in secured areas (including air traffic control operations areas) to ensure the security of passengers and aircraft by January 31, 2001.''

Subsec. (h). Pub. L. 107–71, §144, which directed that subsec. (h) relating to limitation on liability for acts to thwart criminal violence or aircraft piracy be added at end of section 44903, without specifying the Code title to be amended, was executed by making the addition at the end of this section, to reflect the probable intent of Congress.

Pub. L. 107–71, §126(b), added subsec. (h) relating to authority to arm flight deck crews with less-than-lethal weapons.

Pub. L. 107–71, §106(a), added subsec. (h) relating to improved airport perimeter access security.

Subsec. (i). Pub. L. 107–71, §136, added subsec. (i).

2000—Subsec. (c)(2)(C). Pub. L. 106–528, §6, added subpar. (C).

Subsec. (f). Pub. L. 106–181 added subsec. (f).

Subsec. (g). Pub. L. 106–528, §4, added subsec. (g).

EFFECTIVE DATE OF 2012 AMENDMENT

Pub. L. 112–86, §2(b), Jan. 3, 2012, 125 Stat. 1875, provided that: ''Not later than 180 days after the date of enactment of this Act [Jan. 3, 2012], the Assistant Secretary shall implement the plan required by this Act [amending this section and enacting provisions set out as a note under section 40101 of this title].''

EFFECTIVE DATE OF 2003 AMENDMENT

Amendment by Pub. L. 108–176 applicable only to fiscal years beginning after Sept. 30, 2003, except as otherwise specifically provided, see section 3 of Pub. L. 108–176, set out as a note under section 106 of this title.

EFFECTIVE DATE OF 2002 AMENDMENT

Amendment by Pub. L. 107–296 effective 60 days after Nov. 25, 2002, see section 4 of Pub. L. 107–296, set out as an Effective Date note under section 101 of Title 6, Domestic Security.

EFFECTIVE DATE OF 2000 AMENDMENTS

Amendment by Pub. L. 106–528 effective 30 days after Nov. 22, 2000, see section 9 of Pub. L. 106–528, set out as a note under section 106 of this title.

Amendment by Pub. L. 106–181 applicable only to fiscal years beginning after Sept. 30, 1999, see section 3 of

Pub. L. 106–181, set out as a note under section 106 of this title.

SECONDARY COCKPIT BARRIERS

Pub. L. 115–254, div. B, title III, § 336, Oct. 5, 2018, 132 Stat. 3281, provided that:

''(a) SHORT TITLE.—This section may be cited as the 'Saracini Aviation Safety Act of 2018'.

''(b) REQUIREMENT.—Not later than 1 year after the date of the enactment of this Act [Oct. 5, 2018], the Administrator of the Federal Aviation Administration shall issue an order requiring installation of a secondary cockpit barrier on each new aircraft that is manufactured for delivery to a passenger air carrier in the United States operating under the provisions of part 121 of title 14, Code of Federal Regulations.''

SEXUAL MISCONDUCT ONBOARD AIRCRAFT

Pub. L. 115–254, div. B, title III, §§ 339A, 339B, Oct. 5, 2018, 132 Stat. 3282, 3283, provided that:

''SEC. 339A. NATIONAL IN-FLIGHT SEXUAL MISCONDUCT TASK FORCE.

''(a) ESTABLISHMENT OF TASK FORCE.—The Secretary of Transportation shall establish a task force, to be known as the 'National In-Flight Sexual Misconduct Task Force' (referred to in this section as 'Task Force') to—

''(1) review current practices, protocols and requirements of air carriers in responding to allegations of sexual misconduct by passengers onboard aircraft, including training, reporting and data collection; and

''(2) provide recommendations on training, reporting and data collection regarding allegations of sexual misconduct occurring on passenger airline flights that are informed by the review of information described in paragraph (1) and subsection (c)(5) on passengers who have experienced sexual misconduct onboard aircraft.

''(b) MEMBERSHIP.—The Task Force shall be composed of, at a minimum, representatives from—

''(1) [the] Department of Transportation;

''(2) [the] Department of Justice, including the Federal Bureau of Investigation, Office of Victims for Crimes [sic], and the Office on Violence Against Women;

''(3) National organizations that specialize in providing services to sexual assault victims;

''(4) labor organizations that represent flight attendants;

''(5) labor organizations that represent pilots;

''(6) airports;

''(7) air carriers;

''(8) State and local law enforcement agencies; and

''(9) such other Federal agencies and stakeholder organizations as the Secretary of Transportation considers appropriate.

''(c) PURPOSE OF TASK FORCE.—The purpose of the Task Force shall be to—

''(1) issue recommendations for addressing allegations of sexual misconduct by passengers onboard aircraft, including airline employee and contractor training;

''(2) issue recommendations on effective ways for passengers involved in incidents of alleged sexual misconduct to report such allegation of sexual misconduct;

''(3) issue recommendations on how to most effectively provide data on instances of alleged sexual misconduct onboard aircraft and to whom the data collected should be reported in a manner that protects the privacy and confidentiality of individuals involved in incidents of alleged sexual misconduct and precludes the release of data that publically identifies an individual air carrier to enable better understanding of the frequency and severity of such misconduct;

''(4) issue recommendations for flight attendants, pilots, and other appropriate airline personnel on law enforcement notification in incidents of alleged sexual misconduct;

''(5) review and utilize first-hand accounts from passengers who have experienced sexual misconduct onboard aircraft; and

''(6) other matters deemed necessary by the Task Force.

''(d) REPORT.—Not later than 1 year after the date of enactment of this Act [Oct. 5, 2018], the Task Force shall submit a report with its recommendations and findings developed pursuant to subsection (c) to the Secretary of Transportation.

''(e) PLAN.—Not later than 180 days after receiving the report required under subsection (d)[,] the Secretary of Transportation, in coordination with relevant federal agencies, shall submit to [the] appropriate committees of Congress [Committee on Commerce, Science, and Transportation of the Senate and Committee on Transportation and Infrastructure of the House of Representatives] a plan to address the recommendations in the report required under subsection (d). The Secretary of Transportation shall make changes to guidance, policies and regulations, as necessary, within 1 year of submitting the plan required in this subsection.

''(f) REGULATIONS.—Not later than 1 year after submitting the plan required in this subsection [probably means ''subsection (e)''], the Secretary of Transportation may issue regulations as deemed necessary to require each air carrier and other covered entity to develop a policy concerning sexual misconduct in accordance with the recommendations and findings of the Task Force under subsection (c).

''(g) SUNSET.—The Task Force established pursuant to subsection (a) shall terminate upon the submission of the report pursuant to subsection (d).

''SEC. 339B. REPORTING PROCESS FOR SEXUAL MISCONDUCT ONBOARD AIRCRAFT.

''(a) IN GENERAL.—Not later than two years after the date of the enactment of this Act [Oct. 5, 2018], the Attorney General, in coordination with relevant Federal agencies, shall establish a streamlined process, based on the plan required under section 339A(e) of this Act, for individuals involved in incidents of alleged sexual misconduct onboard aircraft to report such allegations of sexual misconduct to law enforcement in a manner that protects the privacy and confidentiality of individuals involved in such allegations.

''(b) AVAILABILITY OF REPORTING PROCESS.—The process for reporting established under subsection (a) shall be made available to the public on the primary Internet websites of—

''(1) the Office for Victims of Crime and the Office on Violence Against Women of the Department of Justice;

''(2) the Federal Bureau of Investigation; and

''(3) the Department of Transportation.''

EMPLOYEE ASSAULT PREVENTION AND RESPONSE PLANS

Pub. L. 115–254, div. B, title V, § 551, Oct. 5, 2018, 132 Stat. 3378, provided that:

''(a) IN GENERAL.—Not later than 90 days after the date of enactment of this Act [Oct. 5, 2018], each air carrier operating under part 121 of title 14, Code of Federal Regulations (in this section referred to as a 'part 121 air carrier'), shall submit to the Administrator [of the Federal Aviation Administration] for review and acceptance an Employee Assault Prevention and Response Plan related to the customer service agents of the air carrier and that is developed in consultation with the labor union representing such agents.

''(b) CONTENTS OF PLAN.—An Employee Assault Prevention and Response Plan submitted under subsection (a) shall include the following:

''(1) Reporting protocols for air carrier customer service agents who have been the victim of a verbal or physical assault.

''(2) Protocols for the immediate notification of law enforcement after an incident of verbal or physical assault committed against an air carrier customer service agent.

''(3) Protocols for informing Federal law enforcement with respect to violations of section 46503 of title 49, United States Code.

''(4) Protocols for ensuring that a passenger involved in a violent incident with a customer service agent of an air carrier is not allowed to move through airport security or board an aircraft until appropriate law enforcement has had an opportunity to assess the incident and take appropriate action.

''(5) Protocols for air carriers to inform passengers of Federal laws protecting Federal, airport, and air carrier employees who have security duties within an airport.

''(c) EMPLOYEE TRAINING.—A part 121 air carrier shall conduct initial and recurrent training for all employees, including management, of the air carrier with respect to the plan required under subsection (a), which shall include training on de-escalating hostile situations, written protocols on dealing with hostile situations, and the reporting of relevant incidents.

''(d) STUDY.—Not later than 180 days after the date of enactment of this Act, the Comptroller General of the United States shall—

''(1) complete a study of crimes of violence (as defined in section 16 of title 18, United States Code) committed against airline customer service representatives while they are performing their duties and on airport property; and

''(2) submit the findings of the study, including any recommendations, to the appropriate committees of Congress [Committee on Commerce, Science, and Transportation of the Senate and Committee on Transportation and Infrastructure of the House of Representatives].

''(e) GAP ANALYSIS.—The study required under subsection (d) shall include a gap analysis to determine if State and local laws and resources are adequate to deter or otherwise address the crimes of violence described in subsection (a) and recommendations on how to address any identified gaps.''

TRANSPORTATION SECURITY LABORATORY

Pub. L. 115–254, div. K, title I, §1915, Oct. 5, 2018, 132 Stat. 3555, provided that:

''(a) IN GENERAL.—Not later than 1 year after the date of enactment of this Act [Oct. 5, 2018], the Secretary [of Homeland Security], in consultation with the Administrator [of the Transporation Security Administration] and the Undersecretary for Science and Technology—

''(1) shall conduct a review to determine whether the TSA [Transportation Security Administration] is the most appropriate component within the Department [of Homeland Security] to administer the Transportation Security Laboratory; and

''(2) may direct the TSA to administer the Transportation Security Laboratory if the review under paragraph (1) identifies the TSA as the most appropriate component.

''(b) PERIODIC REVIEWS.—The Secretary shall periodically review the screening technology test and evaluation process conducted at the Transportation Security Laboratory to improve the coordination, collaboration, and communication between the Transportation Security Laboratory and the TSA to identify factors contributing to acquisition inefficiencies, develop strategies to reduce acquisition inefficiencies, facilitate more expeditious initiation and completion of testing, and identify how laboratory practices can better support acquisition decisions.

''(c) REPORTS.—The Secretary shall report the findings of each review under this section to the appropriate committees of Congress [Committees on Commerce, Science, and Transportation and Homeland Security and Governmental Affairs of the Senate and Committee on Homeland Security of the House of Representatives].''

PILOT PROGRAM FOR AUTOMATED EXIT LANE TECHNOLOGY

Pub. L. 115–254, div. K, title I, §1920, Oct. 5, 2018, 132 Stat. 3560, provided that:

''(a) IN GENERAL.—Not later than 90 days after the date of enactment of this Act [Oct. 5, 2018], the Administrator [of the Transportation Security Administration] shall establish a pilot program to implement and evaluate the use of automated exit lane technology at small hub airports and nonhub airports (as those terms are defined in section 40102 of title 49, United States Code).

''(b) PARTNERSHIP.—The Administrator shall carry out the pilot program in partnership with the applicable airport directors.

''(c) COST SHARE.—The Federal share of the cost of the pilot program under this section shall not exceed 85 percent of the total cost of the program.

''(d) AUTHORIZATION OF APPROPRIATIONS.—There is authorized to be appropriated to carry out the pilot program under this section $15,000,000 for each of fiscal years 2019 through 2021.

''(e) GAO REPORT.—Not later than 2 years after the date the pilot program is implemented, the Comptroller General of the United States shall submit to the appropriate committees of Congress [Committees on Commerce, Science, and Transportation and Homeland Security and Governmental Affairs of the Senate and Committee on Homeland Security of the House of Representatives] a report on the pilot program, including—

''(1) the extent of airport participation in the pilot program and how the program was implemented;

''(2) the results of the pilot program and any reported benefits, including the impact on security and any cost-related efficiencies realized by TSA [Transportation Security Administration] or at the participating airports; and

''(3) the feasibility of expanding the pilot program to additional airports, including to medium and large hub airports.''

SECURING AIRPORT WORKER ACCESS POINTS

Pub. L. 115–254, div. K, title I, §1934, Oct. 5, 2018, 132 Stat. 3572, provided that:

''(a) COOPERATIVE EFFORTS TO ENHANCE AIRPORT SECURITY AWARENESS.—Not later than 180 days after the date of enactment of this Act [Oct. 5, 2018], the Administrator shall consult with air carriers, foreign air carriers, airport operators, and labor unions representing credentialed employees to enhance security awareness of credentialed airport populations regarding insider threats to aviation security and best practices related to airport access controls.

''(b) CREDENTIALING STANDARDS.—Not later than 180 days after the date of enactment of this Act, the Administrator, in consultation with air carriers, foreign air carriers, airport operators, and labor unions representing credentialed employees, shall assess credentialing standards, policies, and practices, including implementation of relevant credentialing updates required under the FAA Extension, Safety, and Security Act of 2016 (Public Law 114–190; 130 Stat. 615) [see Tables for classification], to ensure that insider threats to aviation security are adequately addressed.

''(c) SIDA APPLICATIONS.—

''(1) SOCIAL SECURITY NUMBERS REQUIRED.—

''(A) IN GENERAL.—Not later than 60 days after the date of enactment of this Act, the Administrator shall revise the application submitted by an individual applying for a credential granting access to the Secure Identification Area of an airport to require the social security number of such individual in order to strengthen security vetting effectiveness.

''(B) FAILURE TO PROVIDE NUMBER.—An applicant who does not provide such applicant's social security number may be denied such a credential.

''(2) SCREENING NOTICE.—The Administrator shall issue requirements for an airport operator to include in each application for access to a Security Identification Display Area notification to the applicant that an employee holding a credential granting access to a Security Identification Display Area may be screened at any time while gaining access to, work-

ing in, or leaving a Security Identification Display Area.

''(d) SECURED AND STERILE AREAS OF AIRPORTS.—The Administrator shall consult with airport operators and airline operators to identify advanced technologies, including biometric identification technologies, that could be used for securing employee access to the secured areas and sterile areas of airports.

''(e) RAP BACK VETTING .—Not later than 180 days after the date of enactment of this Act, the Administrator shall identify and submit to the appropriate committees of Congress the number of credentialed aviation worker populations at airports that are continuously vetted through the Federal Bureau of Investigation's Rap Back Service, consistent with section 3405(b)(2) of the FAA Extension, Safety, and Security Act of 2016 (49 U.S.C. 44901 note).

''(f) INSIDER THREAT EDUCATION AND MITIGATION.—Not later than 180 days after the date of enactment of this Act, the Administrator shall identify means of enhancing the TSA's ability to leverage the resources of the Department and the intelligence community (as defined in section 3 of the National Security Act of 1947 (50 U.S.C. 3003)) to educate Administration personnel on insider threats to aviation security and how the TSA can better mitigate such insider threats.

''(g) EMPLOYEE INSPECTIONS.—Consistent with the FAA Extension, Safety, and Security Act of 2016 (Public Law 114–190; 130 Stat. 615), the Administrator shall ensure that TSA-led, random employee physical inspection efforts of aviation workers are targeted, strategic, and focused on providing the greatest level of security effectiveness.

''(h) COVERT TESTING.—

''(1) IN GENERAL.—Consistent with the FAA Extension, Safety, and Security Act of 2016 (Public Law 114–190; 130 Stat. 615), the Administrator shall continue to conduct covert testing of TSA-led employee inspection operations at airports and measure existing levels of security effectiveness.

''(2) REQUIREMENTS.—The Administrator shall provide—

''(A) the results of such testing to—

''(i) the airport operator for the airport that is the subject of any such testing; and

''(ii) as appropriate, to air carriers and foreign air carriers that operate at the airport that is the subject of such testing; and

''(B) recommendations and technical assistance for air carriers, foreign air carriers, and airport operators to conduct their own employee inspections, as needed.

''(3) ANNUAL REPORTING.—The Administrator shall for each of fiscal years 2019 through 2021, submit to the appropriate committees of Congress a report on the frequency, methodology, strategy, and effectiveness of employee inspection operations at airports.

''(i) CENTRALIZED DATABASE.—

''(1) IN GENERAL.—Not later than 180 days after the date of enactment of this Act [Oct. 5, 2018], the Administrator, in consultation with ASAC, shall—

''(A) subject to paragraph (2), establish a national, centralized database of the names of each individual who—

''(i) has had an airport-issued badge revoked for failure to comply with aviation security requirements; or

''(ii) has had an aircraft operator-issued badge revoked for failure to comply with aviation security requirements;

''(B) determine the appropriate reporting mechanisms for air carriers, foreign air carriers, and airport operators—

''(i) to submit to the Administration data regarding an individual described in subparagraph (A); and

''(ii) to access the database; and

''(C) establish a process to allow an individual whose name is mistakenly entered into the database to correct the record and have the individual's name expunged from the database.

''(2) LIMITATION.—The database shall not include the name of any individual whose badge has been revoked as a result of a termination or cessation of employment unrelated to—

''(A) a violation of a security requirement; or

''(B) a determination that the individual poses a threat to aviation security.''

[For definitions of terms used in section 1934 of Pub. L. 115–254, set out above, see section 1902 of Pub. L. 115–254, set out as a Definitions of Terms in Title I of Div. K of Pub. L. 115–254 note under section 101 of this title.]

LAW ENFORCEMENT OFFICER REIMBURSEMENT PROGRAM

Pub. L. 115–254, div. K, title I, § 1935, Oct. 5, 2018, 132 Stat. 3574, provided that:

''(a) IN GENERAL.—In accordance with section 44903(c)(1) of title 49, United States Code, the Administrator [of the Transportation Security Administration] shall increase the number of awards, and the total funding amount of each award, under the Law Enforcement Officer Reimbursement Program—

''(1) to increase the presence of law enforcement officers in the public areas of airports, including baggage claim, ticket counters, and nearby roads;

''(2) to increase the presence of law enforcement officers at screening checkpoints;

''(3) to reduce the response times of law enforcement officers during security incidents; and

''(4) to provide visible deterrents to potential terrorists.

''(b) COOPERATION BY ADMINISTRATOR.—In carrying out subsection (a), the Administrator shall use the authority provided to the Administrator under section 114(m) of title 49, United States Code, that is the same authority as is provided to the Administrator of the Federal Aviation Administration under section 106(m) of that title.

''(c) ADMINISTRATIVE BURDENS.—The Administrator shall review the regulations and compliance policies related to the Law Enforcement Officer Reimbursement Program and, if necessary, revise such regulations and policies to reduce any administrative burdens on applicants or recipients of such awards.

''(d) AUTHORIZATION OF APPROPRIATIONS.—There is authorized to be appropriated to carry out section 44901(h) of title 49, United States Code, $55,000,000 for each of fiscal years 2019 through 2021.''

AIRPORT PERIMETER AND ACCESS CONTROL SECURITY

Pub. L. 115–254, div. K, title I, § 1936, Oct. 5, 2018, 132 Stat. 3575, provided that:

''(a) RISK ASSESSMENTS OF AIRPORT SECURITY.—

''(1) IN GENERAL.—The Administrator [of the Transportation Security Administration] shall—

''(A) not later than 180 days after the date of enactment of this Act [Oct. 5, 2018], update the Transportation Sector Security Risk Assessment (referred to in this section as the 'TSSRA'); and

''(B) not later than 90 days after the date the TSSRA is updated under subparagraph (A)—

''(i) update with the most currently available intelligence information the Comprehensive Risk Assessment of Perimeter and Access Control Security (referred to in this section as the 'Risk Assessment of Airport Security');

''(ii) establish a regular schedule for periodic updates to the Risk Assessment of Airport Security; and

''(iii) conduct a system-wide assessment of airport access control points and airport perimeter security.

''(2) CONTENTS.—The security risk assessments required under paragraph (1)(B) shall—

''(A) include updates reflected in the TSSRA and Joint Vulnerability Assessment findings;

''(B) reflect changes to the risk environment relating to airport access control points and airport perimeters;

''(C) 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

''(D) consider the unique geography of and current best practices used by airports to mitigate potential vulnerabilities.

''(3) REPORT.—The Administrator shall report the results of the TSSRA and Risk Assessment of Airport Security under paragraph (1) to—

''(A) the appropriate committees of Congress [Committees on Commerce, Science, and Transportation and Homeland Security and Governmental Affairs of the Senate and Committee on Homeland Security of the House of Representatives];

''(B) relevant Federal departments and agencies; and

''(C) airport operators.

''(b) AIRPORT SECURITY STRATEGY DEVELOPMENT.—

''(1) IN GENERAL.—Not later than 90 days after the date of enactment of this Act, the Administrator shall update the 2012 National Strategy for Airport Perimeter and Access Control Security (referred to in this section as the 'National Strategy').

''(2) CONTENTS.—The update to the National Strategy shall include—

''(A) information from the Risk Assessment of Airport Security; and

''(B) information on—

''(i) airport security-related activities;

''(ii) the status of TSA [Transportation Security Administration] efforts to address the objectives of the National Strategy;

''(iii) finalized outcome-based performance measures and performance levels for—

''(I) each activity described in clause (i); and

''(II) each objective described in clause (ii); and

''(iv) input from airport operators.

''(3) UPDATES.—Not later than 90 days after the date the update to the National Strategy is complete, the Administrator shall establish a regular schedule for determining if and when additional updates to the strategy under paragraph (1) are necessary.''

TRAVELER REDRESS IMPROVEMENT

Pub. L. 115–254, div. K, title I, §1949, Oct. 5, 2018, 132 Stat. 3588, provided that:

''(a) REDRESS PROCESS.—

''(1) IN GENERAL.—Not later than 30 days after the date of enactment of this Act [Oct. 5, 2018], the Administrator [of the Transportation Security Administration], using existing resources, systems, and processes, shall ensure the availability of the Department of Homeland Security Traveler Redress Inquiry Program (referred to in this section as 'DHS TRIP') redress process to adjudicate an inquiry for an individual who—

''(A) is a citizen of the United States or alien lawfully admitted for permanent residence;

''(B) has filed the inquiry with DHS TRIP after receiving enhanced screening at an airport passenger security checkpoint more than 3 times in any 60-day period; and

''(C) believes the individual has been wrongly identified as being a threat to aviation security.

''(2) BRIEFING.—Not later than 180 days after the date of enactment of this Act, the Administrator shall brief the appropriate committees of Congress [Committees on Commerce, Science, and Transportation and Homeland Security and Governmental Affairs of the Senate and Committee on Homeland Security of the House of Representatives] on the implementation of the redress process required under paragraph (1).

''(b) PRIVACY IMPACT REVIEW AND UPDATE.—

''(1) IN GENERAL.—Not later than 180 days after the date of enactment of this Act, the Administrator shall review and update the Privacy Impact Assessment for the Secure Flight programs to ensure the assessment accurately reflects the operation of such programs.

''(2) PUBLIC DISSEMINATION; FORM.—The Administrator shall—

''(A) publish the Secure Flight Privacy Impact Assessment review and update required under paragraph (1) on a publicly-accessible internet webpage of the TSA [Transportation Security Administration]; and

''(B) submit the Secure Flight Privacy Impact Assessment review and update to the appropriate committees of Congress.

''(c) RULE REVIEW AND NOTIFICATION PROCESS.—

''(1) RULE REVIEW.—Not later than 60 days after the date of enactment of this Act, and every 120 days thereafter, the Assistant Administrator of the Office of Intelligence and Analysis of the TSA, in coordination with the entities specified in paragraph (3), shall identify and review the screening rules established by the Office of Intelligence and Analysis of [the] TSA.

''(2) NOTIFICATION PROCESS.—Not later than 2 days after the date that any change to a rule identified under paragraph (1) is made, the Assistant Administrator of the Office of Intelligence and Analysis of the TSA shall notify the entities specified in paragraph (3) of the change.

''(3) ENTITIES SPECIFIED.—The entities specified in this paragraph are as follows:

''(A) The Office of Civil Rights and Liberties, Ombudsman, and Traveler Engagement of the TSA.

''(B) The Office of Civil Rights and Liberties of the Department [of Homeland Security].

''(C) The Office of Chief Counsel of the TSA.

''(D) The Office of General Counsel of the Department.

''(E) The Privacy Office of the Administration.

''(F) The Privacy Office of the Department.

''(G) The Federal Air Marshal Service.

''(H) The Traveler Redress Inquiry Program of the Department.

''(d) FEDERAL AIR MARSHAL SERVICE COORDINATION.—

''(1) IN GENERAL.—The Administrator shall ensure that the rules identified in subsection (c) are taken into account for Federal Air Marshal mission scheduling.

''(2) REPORT.—Not later than 180 days after the date of enactment of this Act [Oct. 5, 2018], the Administrator shall submit to the appropriate committees of Congress a report on whether, and if so how, the rules identified in subsection (c) are incorporated in the risk analysis conducted during the Federal Air Marshal mission scheduling process.

''(e) GAO REPORT.—Not later than 1 year after the date of enactment of this Act, the Comptroller General of the United States shall—

''(1) study the rules identified under subsection (c)(1), including—

''(A) whether the rules are effective in mitigating potential threats to aviation security; and

''(B) whether, and if so how, the TSA coordinates with the Department regarding any proposed change to a rule; and

''(2) submit to the appropriate committees of Congress a report on the findings under paragraph (1), including any recommendations.''

GENERAL AVIATION AIRPORTS

Pub. L. 115–254, div. K, title I, §1952, Oct. 5, 2018, 132 Stat. 3592, provided that:

''(a) SHORT TITLE.—This section may be cited as the 'Securing General Aviation and Charter Air Carrier Service Act'.

''(b) ADVANCED PASSENGER PRESCREENING SYSTEM.—Not later than 120 days after the date of enactment of this Act [Oct. 5, 2018], the Administrator shall submit to the appropriate committees of Congress a report on the status of the deployment of the advanced passenger prescreening system, and access thereto for certain aircraft charter operators, as required by section 44903(j)(2)(E) of title 49, United States Code, including—

''(1) the reasons for the delay in deploying the system; and

''(2) a detailed schedule of actions necessary for the deployment of the system.

''(c) SCREENING SERVICES OTHER THAN IN PRIMARY PASSENGER TERMINALS.—

''(1) IN GENERAL.—Subject to the provisions of this subsection, the Administrator may provide screening services to a charter air carrier in an area other than the primary passenger terminal of an applicable airport.

''(2) REQUESTS.—A request for screening services under paragraph (1) shall be made at such time, in such form, and in such manner as the Administrator may require, except that the request shall be made to the Federal Security Director for the applicable airport at which the screening services are requested.

''(3) AVAILABILITY.—A Federal Security Director may provide requested screening services under this section if the Federal Security Director determines such screening services are available.

''(4) AGREEMENTS.—

''(A) LIMITATION.—No screening services may be provided under this section unless a charter air carrier agrees in writing to compensate the TSA for all reasonable costs, including overtime, of providing the screening services.

''(B) PAYMENTS.—Notwithstanding section 3302 of title 31, United States Code, payment received under subparagraph (A) shall be credited to the account that was used to cover the cost of providing the screening services. Amounts so credited shall be merged with amounts in that account, and shall be available for the same purposes, and subject to the same conditions and limitations, as other amounts in that account.

''(5) DEFINITIONS.—In this subsection:

''(A) APPLICABLE AIRPORT.—The term 'applicable airport' means an airport that—

''(i) is not a commercial service airport; and

''(ii) is receiving screening services for scheduled passenger aircraft.

''(B) CHARTER AIR CARRIER.—The term 'charter air carrier' has the meaning given the term in section 40102 of title 49, United States Code.

''(C) SCREENING SERVICES.—The term 'screening services' means the screening of passengers and property similar to the screening of passengers and property described in section 44901 of title 49, United States Code.

''(d) REPORT.—Not later than 120 days after the date of enactment of this Act, the Administrator, in consultation with the ASAC, shall, consistent with the requirements of paragraphs (6) and (7) of section 44946(b) of title 49, United States Code, submit to the appropriate Committees of Congress an implementation plan, including an implementation schedule, for any of the following recommendations that were adopted by the ASAC and with which the Administrator has concurred before the date of the enactment of this Act:

''(1) The recommendation regarding general aviation access to Ronald Reagan Washington National Airport, as adopted on February 17, 2015.

''(2) The recommendation regarding the vetting of persons seeking flight training in the United States, as adopted on July 28, 2016.

''(3) Any other such recommendations relevant to the security of general aviation adopted before the date of the enactment of this Act.

''(e) DESIGNATED STAFFING.—The Administrator may designate 1 or more full-time employees of the TSA to liaise with, and respond to issues raised by, general aviation stakeholders.

''(f) SECURITY ENHANCEMENTS.—Not later than 1 year after the date of enactment of this Act, the Administrator, in consultation with the ASAC, shall submit to the appropriate committees of Congress a report on the feasibility of requiring a security threat assessment before an individual could obtain training from a private flight school to operate an aircraft having a maximum certificated takeoff weight of more than 12,500 pounds.''

[For definitions of terms used in section 1952 of Pub. L. 115–254, set out above, see section 1902 of Pub. L. 115–254, set out as a Definitions of Terms in Title I of Div. K of Pub. L. 115–254 note under section 101 of this title.]

FLIGHT DECK SAFETY AND SECURITY

Pub. L. 115–254, div. K, title I, §1961, Oct. 5, 2018, 132 Stat. 3600, provided that:

''(a) THREAT ASSESSMENT.—Not later than 90 days after the date of enactment of this Act [Oct. 5, 2018], the Administrator [of the Transportation Security Administration], in consultation with the Administrator of the Federal Aviation Administration, shall complete a detailed threat assessment to identify any safety or security risks associated with unauthorized access to the flight decks on commercial aircraft and any appropriate measures that should be taken based on the risks.

''(b) RTCA REPORT.—The Administrator, in coordination with the Administrator of the Federal Aviation Administration, shall disseminate RTCA Document (DO–329) Aircraft Secondary Barriers and Alternative Flight Deck Security Procedure to aviation stakeholders, including air carriers and flight crew, to convey effective methods and best practices to protect the flight deck.''

AVIATION CYBERSECURITY

Pub. L. 115–254, div. B, title V, §509, Oct. 5, 2018, 132 Stat. 3355, provided that:

''(a) IN GENERAL.—Not later than 1 year after the date of enactment of this Act [Oct. 5, 2018], the Administrator [of the Federal Aviation Administration] shall initiate a review of the comprehensive and strategic framework of principles and policies (referred to in this section as the 'framework') developed pursuant to section 2111 of the FAA Extension, Safety, and Security Act of 2016 [Pub. L. 114–190] (49 U.S.C. 44903 note) [set out below].

''(b) CONTENTS.—In undertaking the review under subsection (a), the Administrator shall—

''(1) assess the degree to which the framework identifies and addresses known cybersecurity risks associated with the aviation system;

''(2) review existing short- and long-term objectives for addressing cybersecurity risks to the national airspace system; and

''(3) assess the [Federal Aviation] Administration's level of engagement and coordination with aviation stakeholders and other appropriate agencies, organizations, or groups with which the Administration consults to carry out the framework.

''(c) UPDATES.—Upon completion of the review under subsection (a), the Administrator shall modify the framework, as appropriate, to address any deficiencies identified by the review.

''(d) REPORT TO CONGRESS.—Not later than 180 days after initiating the review required by subsection (a), the Administrator shall submit to the appropriate committees of Congress [Committee on Commerce, Science, and Transportation of the Senate and Committee on Transportation and Infrastructure of the House of Representatives] a report on the results of the review, including a description of any modifications made to the framework.''

Pub. L. 114–190, title II, §2111, July 15, 2016, 130 Stat. 625, provided that:

''(a) COMPREHENSIVE AND STRATEGIC AVIATION FRAMEWORK.—

''(1) IN GENERAL.—Not later than 240 days after the date of enactment of this Act [July 15, 2016], the Administrator of the Federal Aviation Administration shall facilitate and support the development of a comprehensive and strategic framework of principles and policies to reduce cybersecurity risks to the national airspace system, civil aviation, and agency information systems using a total systems approach that takes into consideration the interactions and

interdependence of different components of aircraft systems and the national airspace system.

''(2) SCOPE.—In carrying out paragraph (1), the Administrator shall—

''(A) identify and address the cybersecurity risks associated with—

''(i) the modernization of the national airspace system;

''(ii) the automation of aircraft, equipment, and technology; and

''(iii) aircraft systems, including by—

''(I) directing the Aircraft Systems Information Security Protection Working Group—

''(aa) to assess cybersecurity risks to aircraft systems;

''(bb) to review the extent to which existing rulemaking, policy, and guidance to promote safety also promote aircraft systems information security protection; and

''(cc) to provide appropriate recommendations to the Administrator if separate or additional rulemaking, policy, or guidance is needed to address cybersecurity risks to aircraft systems; and

''(II) identifying and addressing—

''(aa) cybersecurity risks associated with in-flight entertainment systems; and

''(bb) whether in-flight entertainment systems can and should be isolated and separate, such as through an air gap, under existing rulemaking, policy, and guidance;

''(B) clarify cybersecurity roles and responsibilities of offices and employees of the Federal Aviation Administration, as the roles and responsibilities relate to cybersecurity at the Federal Aviation Administration;

''(C) identify and implement objectives and actions to reduce cybersecurity risks to air traffic control information systems, including actions to improve implementation of information security standards, such as those of the National Institute of Standards and Technology;

''(D) support voluntary efforts by industry, RTCA, Inc., and other standards-setting organizations to develop and identify consensus standards and best practices relating to guidance on aviation systems information security protection, consistent, to the extent appropriate, with the cybersecurity risk management activities described in section 2(e) of the National Institute of Standards and Technology Act (15 U.S.C. 272(e));

''(E) establish guidelines for the voluntary exchange of information between and among aviation stakeholders pertaining to aviation-related cybersecurity incidents, threats, and vulnerabilities;

''(F) identify short- and long-term objectives and actions that can be taken in response to cybersecurity risks to the national airspace system; and

''(G) identify research and development activities to inform actions in response to cybersecurity risks.

''(3) IMPLEMENTATION REQUIREMENTS.—In carrying out the activities under this subsection, the Administrator shall—

''(A) coordinate with aviation stakeholders, including, at a minimum, representatives of industry, airlines, manufacturers, airports, RTCA, Inc., and unions;

''(B) consult with the heads of relevant agencies and with international regulatory authorities;

''(C) if determined appropriate, convene an expert panel or working group to identify and address cybersecurity risks; and

''(D) evaluate, on a periodic basis, the effectiveness of the principles established under this subsection.

''(b) UPDATE ON CYBERSECURITY IMPLEMENTATION PROGRESS.—Not later than 90 days after the date of enactment of this Act [July 15, 2016], the Administrator shall provide to the appropriate committees of Congress [Committee on Commerce, Science, and Transportation of the Senate and Committee on Transportation and Infrastructure of the House of Representatives] an update on progress made toward the implementation of this section.

''(c) CYBERSECURITY THREAT MODEL.—Not later than 1 year after the date of enactment of this Act, the Administrator, in consultation with the Director of the National Institute of Standards and Technology, shall implement the open recommendation issued in 2015 by the Government Accountability Office to assess and research the potential cost and timetable of developing and maintaining an agencywide threat model, which shall be updated regularly, to strengthen the cybersecurity of agency systems across the Federal Aviation Administration. The Administrator shall brief the Committee on Science, Space, and Technology and the Committee on Transportation and Infrastructure of the House of Representatives and the Committee on Commerce, Science, and Transportation of the Senate on the status, results, and composition of the threat model.

''(d) NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY INFORMATION SECURITY STANDARDS.—Not later than 180 days after the date of enactment of this Act, the Administrator of the Federal Aviation Administration, after consultation with the Director of the National Institute of Standards and Technology, shall transmit to the Committee on Science, Space, and Technology and the Committee on Transportation and Infrastructure of the House of Representatives and the Committee on Commerce, Science, and Transportation of the Senate a report on—

''(1) a cybersecurity standards plan to improve implementation of the National Institute of Standards and Technology's latest revisions to information security guidance for Federal Aviation Administration information and Federal Aviation Administration information systems within set timeframes; and

''(2) an explanation of why any such revisions are not incorporated in the plan or are not incorporated within set timeframes.

''(e) CYBERSECURITY RESEARCH AND DEVELOPMENT.—Not later than 1 year after the date of enactment of this Act, the Administrator, in consultation with other agencies as appropriate, shall establish a cybersecurity research and development plan for the national airspace system, including—

''(1) any proposal for research and development cooperation with international partners;

''(2) an evaluation and determination of research and development needs to determine any cybersecurity risks of cabin communications and cabin information technology systems on board in the passenger domain; and

''(3) objectives, proposed tasks, milestones, and a 5-year budgetary profile.''

AIRPORT SECURITY

Pub. L. 114–50, Sept. 24, 2015, 129 Stat. 490, provided that:

''SECTION 1. SHORT TITLE.

''This Act may be cited as the 'Gerardo Hernandez Airport Security Act of 2015'.

''SEC. 2. DEFINITIONS.

''In this Act:

''(1) ASSISTANT SECRETARY.—The term 'Assistant Secretary' means the Assistant Secretary of Homeland Security (Transportation Security) of the Department of Homeland Security.

''(2) ADMINISTRATION.—The term 'Administration' means the Transportation Security Administration.

''SEC. 3. SECURITY INCIDENT RESPONSE AT AIRPORTS.

''(a) IN GENERAL.—The Assistant Secretary shall, in consultation with other Federal agencies as appro-

priate, conduct outreach to all airports in the United States at which the Administration performs, or oversees the implementation and performance of, security measures, and provide technical assistance as necessary, to verify such airports have in place individualized working plans for responding to security incidents inside the perimeter of the airport, including active shooters, acts of terrorism, and incidents that target passenger-screening checkpoints.

''(b) TYPES OF PLANS.—Such plans may include, but may not be limited to, the following:

''(1) A strategy for evacuating and providing care to persons inside the perimeter of the airport, with consideration given to the needs of persons with disabilities.

''(2) A plan for establishing a unified command, including identification of staging areas for non-airport-specific law enforcement and fire response.

''(3) A schedule for regular testing of communications equipment used to receive emergency calls.

''(4) An evaluation of how emergency calls placed by persons inside the perimeter of the airport will reach airport police in an expeditious manner.

''(5) A practiced method and plan to communicate with travelers and all other persons inside the perimeter of the airport.

''(6) To the extent practicable, a projected maximum timeframe for law enforcement response to active shooters, acts of terrorism, and incidents that target passenger security-screening checkpoints.

''(7) A schedule of joint exercises and training to be conducted by the airport, the Administration, other stakeholders such as airport and airline tenants, and any relevant law enforcement, airport police, fire, and medical personnel.

''(8) A schedule for producing after-action joint exercise reports to identify and determine how to improve security incident response capabilities.

''(9) A strategy, where feasible, for providing airport law enforcement with access to airport security video surveillance systems at category X airports where those systems were purchased and installed using Administration funds.

''(c) REPORT TO CONGRESS.—Not later than 180 days after the date of the enactment of this Act [Sept. 24, 2015], the Assistant Secretary 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 findings from its outreach to airports under subsection (a), including an analysis of the level of preparedness such airports have to respond to security incidents, including active shooters, acts of terrorism, and incidents that target passenger-screening checkpoints.

''SEC. 4. DISSEMINATING INFORMATION ON BEST PRACTICES.

''The Assistant Secretary shall—

''(1) identify best practices that exist across airports for security incident planning, management, and training; and

''(2) establish a mechanism through which to share such best practices with other airport operators nationwide.

''SEC. 5. CERTIFICATION.

''Not later than 90 days after the date of enactment of this Act [Sept. 24, 2015], and annually thereafter, the Assistant Secretary shall certify in writing to the Committee on Homeland Security of the House of Representatives and the Committee on Commerce, Science, and Transportation of the Senate that all screening personnel have participated in practical training exercises for active shooter scenarios.

''SEC. 6. REIMBURSABLE AGREEMENTS.

''Not later than 90 days after the enactment of this Act [Sept. 24, 2015], the Assistant Secretary shall provide to the Committee on Homeland Security of the House of Representatives and the Committee on Commerce, Science, and Transportation of the Senate an analysis of how the Administration can use cost savings achieved through efficiencies to increase over the next 5 fiscal years the funding available for checkpoint screening law enforcement support reimbursable agreements.

''SEC. 7. SECURITY INCIDENT RESPONSE FOR SURFACE TRANSPORTATION SYSTEMS.

''(a) IN GENERAL.—The Assistant Secretary shall, in consultation with the Secretary of Transportation, and other relevant agencies, conduct outreach to all passenger transportation agencies and providers with high-risk facilities, as identified by the Assistant Secretary, to verify such agencies and providers have in place plans to respond to active shooters, acts of terrorism, or other security-related incidents that target passengers.

''(b) TYPES OF PLANS.—As applicable, such plans may include, but may not be limited to, the following:

''(1) A strategy for evacuating and providing care to individuals, with consideration given to the needs of persons with disabilities.

''(2) A plan for establishing a unified command.

''(3) A plan for frontline employees to receive active shooter training.

''(4) A schedule for regular testing of communications equipment used to receive emergency calls.

''(5) An evaluation of how emergency calls placed by individuals using the transportation system will reach police in an expeditious manner.

''(6) A practiced method and plan to communicate with individuals using the transportation system.

''(c) REPORT TO CONGRESS.—Not later than 180 days after the date of enactment of this Act [Sept. 24, 2015], the Assistant Secretary 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 findings from its outreach to the agencies and providers under subsection (a), including an analysis of the level of preparedness such transportation systems have to respond to security incidents.

''(d) DISSEMINATION OF BEST PRACTICES.—The Assistant Secretary shall identify best practices for security incident planning, management, and training and establish a mechanism through which to share such practices with passenger transportation agencies nationwide.

''SEC. 8. NO ADDITIONAL AUTHORIZATION OF APPROPRIATIONS.

''No additional funds are authorized to be appropriated to carry out this Act, and this Act shall be carried out using amounts otherwise available for such purpose.

''SEC. 9. INTEROPERABILITY REVIEW.

''(a) IN GENERAL.—Not later than 90 days after the date of enactment of this Act [Sept. 24, 2015], the Assistant Secretary shall, in consultation with the Assistant Secretary of the Office of Cybersecurity and Communications, conduct a review of the interoperable communications capabilities of the law enforcement, fire, and medical personnel responsible for responding to a security incident, including active shooter events, acts of terrorism, and incidents that target passenger-screening checkpoints, at all airports in the United States at which the Administration performs, or oversees the implementation and performance of, security measures.

''(b) REPORT.—Not later than 30 days after the completion of the review, the Assistant Secretary shall report the findings of the review to the Committee on Homeland Security of the House of Representatives and the Committee on Commerce, Science, and Transportation of the Senate.''

CABIN FLIGHT CREW PARTICIPATION IN KNOWN CREWMEMBER PILOT PROGRAM

Pub. L. 113–6, div. D, title II, Mar. 26, 2013, 127 Stat. 349, provided in part: ''That the Administrator of the

Transportation Security Administration shall, within 270 days of the date of enactment of this Act [Mar. 26, 2013], establish procedures allowing members of cabin flight crews of air carriers to participate in the Known Crewmember pilot program, unless the Administrator determines that meeting the requirement within this timeline is not practicable and informs the Committees on Appropriations of the Senate and House of Representatives of the basis for that determination and the new timeline for implementing the requirement''.

STRATEGIC PLAN TO TEST AND IMPLEMENT ADVANCED PASSENGER PRESCREENING SYSTEM

Pub. L. 110–53, title XVI, §1605, Aug. 3, 2007, 121 Stat. 481, provided that:

''(a) IN GENERAL.—Not later than 120 days after the date of enactment of this Act [Aug. 3, 2007], the Secretary of Homeland Security, in consultation with the Administrator of the Transportation Security Administration, shall submit to the Committee on Homeland Security of the House of Representatives, the Committee on Commerce, Science, and Transportation of the Senate, and the Committee on Homeland Security and Governmental Affairs of the Senate a plan that—

''(1) describes the system to be utilized by the Department of Homeland Security to assume the performance of comparing passenger information, as defined by the Administrator, to the automatic selectee and no-fly lists, utilizing appropriate records in the consolidated and integrated terrorist watchlist maintained by the Federal Government;

''(2) provides a projected timeline for each phase of testing and implementation of the system;

''(3) explains how the system will be integrated with the prescreening system for passengers on international flights; and

''(4) describes how the system complies with section 552a of title 5, United States Code.

''(b) GAO ASSESSMENT.—Not later than 180 days after the date of enactment of this Act, the Comptroller General shall submit a report to the Committee on Commerce, Science, and Transportation of the Senate and the Committee on Homeland Security of the House of Representatives that—

''(1) describes the progress made by the Transportation Security Administration in implementing the secure flight passenger pre-screening program;

''(2) describes the effectiveness of the current appeals process for passengers wrongly assigned to the no-fly and terrorist watch lists;

''(3) describes the Transportation Security Administration's plan to protect private passenger information and progress made in integrating the system with the pre-screening program for international flights operated by United States Customs and Border Protection;

''(4) provides a realistic determination of when the system will be completed; and

''(5) includes any other relevant observations or recommendations the Comptroller General deems appropriate.''

PILOT PROJECT TO TEST DIFFERENT TECHNOLOGIES AT AIRPORT EXIT LANES

Pub. L. 110–53, title XVI, §1613, Aug. 3, 2007, 121 Stat. 485, provided that:

''(a) IN GENERAL.—The Administrator of the Transportation Security Administration shall conduct a pilot program at not more than 2 airports to identify technologies to improve security at airport exit lanes.

''(b) PROGRAM COMPONENTS.—In conducting the pilot program under this section, the Administrator shall—

''(1) utilize different technologies that protect the integrity of the airport exit lanes from unauthorized entry;

''(2) work with airport officials to deploy such technologies in multiple configurations at a selected airport or airports at which some of the exits are not co-located with a screening checkpoint; and

''(3) ensure the level of security is at or above the level of existing security at the airport or airports where the pilot program is conducted.

''(c) REPORTS.—

''(1) INITIAL BRIEFING.—Not later than 180 days after the date of enactment of this Act [Aug. 3, 2007], the Administrator shall conduct a briefing to the congressional committees set forth in paragraph (3) that describes—

''(A) the airport or airports selected to participate in the pilot program;

''(B) the technologies to be tested;

''(C) the potential savings from implementing the technologies at selected airport exits;

''(D) the types of configurations expected to be deployed at such airports; and

''(E) the expected financial contribution from each airport.

''(2) FINAL REPORT.—Not later than 18 months after the technologies are deployed at the airports participating in the pilot program, the Administrator shall submit a final report to the congressional committees set forth in paragraph (3) that describes—

''(A) the changes in security procedures and technologies deployed;

''(B) the estimated cost savings at the airport or airports that participated in the pilot program; and

''(C) the efficacy and staffing benefits of the pilot program and its applicability to other airports in the United States.

''(3) CONGRESSIONAL COMMITTEES.—The reports required under this subsection shall be submitted to—

''(A) the Committee on Commerce, Science, and Transportation of the Senate;

''(B) the Committee on Appropriations of the Senate;

''(C) the Committee on Homeland Security and Governmental Affairs of the Senate;

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

''(E) the Committee on Appropriations of the House of Representatives.

''(d) USE OF EXISTING FUNDS.—This section shall be executed using existing funds.''

SECURITY CREDENTIALS FOR AIRLINE CREWS

Pub. L. 110–53, title XVI, §1614, Aug. 3, 2007, 121 Stat. 486, provided that:

''(a) REPORT.—Not later than 180 days after the date of enactment of this Act [Aug. 3, 2007], the Administrator of the Transportation Security Administration, after consultation with airline, airport, and flight crew representatives, shall submit to the Committee on Commerce, Science, and Transportation of the Senate, the Committee on Homeland Security and Governmental Affairs of the Senate, the Committee on Homeland Security of the House of Representatives, and the Committee on Transportation and Infrastructure of the House of Representatives a report on the status of the Administration's efforts to institute a sterile area access system or method that will enhance security by properly identifying authorized airline flight deck and cabin crew members at screening checkpoints and granting them expedited access through screening checkpoints. The Administrator shall include in the report recommendations on the feasibility of implementing the system for the domestic aviation industry beginning 1 year after the date on which the report is submitted.

''(b) BEGINNING IMPLEMENTATION.—The Administrator shall begin implementation of the system or method referred to in subsection (a) not later than 1 year after the date on which the Administrator submits the report under subsection (a).''

CAPPS2

Pub. L. 108–176, title VI, §607, Dec. 12, 2003, 117 Stat. 2568, provided that:

''(a) IN GENERAL.—The Under Secretary for Border and Transportation Security of the Department of

Homeland Security shall not implement, on other than a test basis, the computer assisted passenger prescreening system (commonly known as and in this section referred to as 'CAPPS2') until the Under Secretary provides to Congress a certification that—

''(1) a procedure is established enabling airline passengers, who are delayed or prohibited from boarding a flight because CAPPS2 determined that they might pose a security threat, to appeal such determination and correct information contained in CAPPS2;

''(2) the error rate of the Government and private data bases that will be used to both establish identity and assign a risk level to a passenger under CAPPS2 will not produce a large number of false positives that will result in a significant number of passengers being mistaken as a security threat;

''(3) the Under Secretary has demonstrated the efficacy and accuracy of all search tools in CAPPS2 and has demonstrated that CAPPS2 can make an accurate predictive assessment of those passengers who would constitute a security threat;

''(4) the Secretary of Homeland Security has established an internal oversight board to oversee and monitor the manner in which CAPPS2 is being implemented;

''(5) the Under Secretary has built in sufficient operational safeguards to reduce the opportunities for abuse;

''(6) substantial security measures are in place to protect CAPPS2 from unauthorized access by hackers or other intruders;

''(7) the Under Secretary has adopted policies establishing effective oversight of the use and operation of the system; and

''(8) there are no specific privacy concerns with the technological architecture of the system.

''(b) GAO REPORT.—Not later than 90 days after the date on which certification is provided under subsection (a), the Comptroller General shall submit a report to the Committees on Appropriations of the House of Representatives and the Senate, the Committee on Transportation and Infrastructure of the House of Representatives, and the Committee on Commerce, Science and Transportation of the Senate that assesses the impact of CAPPS2 on the issues listed in subsection (a) and on privacy and civil liberties. The report shall include any recommendations for practices, procedures, regulations, or legislation to eliminate or minimize adverse effect of CAPPS2 on privacy, discrimination, and other civil liberties.''

REIMBURSEMENT OF AIR CARRIERS FOR CERTAIN SCREENING AND RELATED ACTIVITIES

Pub. L. 108–176, title VIII, §821, Dec. 12, 2003, 117 Stat. 2594, provided that: ''The Secretary of Homeland Security, subject to the availability of funds (other than amounts in the Aviation Trust Fund) provided for this purpose, shall reimburse air carriers and airports for—

''(1) the screening of catering supplies; and

''(2) checking documents at security checkpoints.''

IMPROVED FLIGHT DECK INTEGRITY MEASURES

Pub. L. 107–71, title I, §104, Nov. 19, 2001, 115 Stat. 605, provided that:

''(a) IN GENERAL.—As soon as possible after the date of enactment of this Act [Nov. 19, 2001], the Administrator of the Federal Aviation Administration shall—

''(1) issue an order (without regard to the provisions of chapter 5 of title 5, United States Code)—

''(A) prohibiting access to the flight deck of aircraft engaged in passenger air transportation or intrastate air transportation that are required to have a door between the passenger and pilot compartments under title 14, Code of Federal Regulations, except to authorized persons;

''(B) requiring the strengthening of the flight deck door and locks on any such aircraft operating in air transportation or intrastate air transportation that has a rigid door in a bulkhead between the flight deck and the passenger area to ensure that the door cannot be forced open from the passenger compartment;

''(C) requiring that such flight deck doors remain locked while any such aircraft is in flight except when necessary to permit access and egress by authorized persons; and

''(D) prohibiting the possession of a key to any such flight deck door by any member of the flight crew who is not assigned to the flight deck; and

''(2) take such other action, including modification of safety and security procedures and flight deck redesign, as may be necessary to ensure the safety and security of the aircraft.

''(b) IMPLEMENTATION OF OTHER METHODS.—As soon as possible after such date of enactment [Nov. 19, 2001], the Administrator of the Federal Aviation Administration may develop and implement methods—

''(1) to use video monitors or other devices to alert pilots in the flight deck to activity in the cabin, except that the use of such monitors or devices shall be subject to nondisclosure requirements applicable to cockpit video recordings under section 1114(c) [of title 49];

''(2) to ensure continuous operation of an aircraft transponder in the event of an emergency; and

''(3) to revise the procedures by which cabin crews of aircraft can notify flight deck crews of security breaches and other emergencies, including providing for the installation of switches or other devices or methods in an aircraft cabin to enable flight crews to discreetly notify the pilots in the case of a security breach occurring in the cabin.

''(c) COMMUTER AIRCRAFT.—The Administrator shall investigate means of securing the flight deck of scheduled passenger aircraft operating in air transportation or intrastate air transportation that do not have a rigid fixed door with a lock between the passenger compartment and the flight deck and issue such an order as the Administrator deems appropriate to ensure the inaccessibility, to the greatest extent feasible, of the flight deck while the aircraft is so operating, taking into consideration such aircraft operating in regions where there is minimal threat to aviation security or national security.''

SMALL AND MEDIUM AIRPORTS

Pub. L. 107–71, title I, §106(b), Nov. 19, 2001, 115 Stat. 609, provided that:

''(1) TECHNICAL SUPPORT AND FINANCIAL ASSISTANCE.—The Under Secretary of Transportation for Security [now Administrator of the Transportation Security Administration] shall develop a plan to—

''(A) provide technical support to airports, each of which had less than 1 percent of the total annual enplanements in the United States for the most recent calendar year for which data is available, to enhance security operations; and

''(B) provide financial assistance to those airports to defray the costs of enhancing security.

''(2) REMOVAL OF CERTAIN RESTRICTIONS.—

''(A) CERTIFICATION BY OPERATOR.—If the operator of an airport described in paragraph (1), after consultation with the appropriate State and local law enforcement authorities, determines that safeguards are in place to sufficiently protect public safety, and so certifies in writing to the Under Secretary, then any security rule, order, or other directive restricting the parking of passenger vehicles shall not apply at that airport after the applicable time period specified in subparagraph (B), unless the Under Secretary, taking into account individual airport circumstances, notifies the airport operator that the safeguards in place do not adequately respond to specific security risks and that the restriction must be continued in order to ensure public safety.

''(B) COUNTERMAND PERIOD.—The time period within which the Secretary may notify an airport operator, after receiving a certification under subparagraph (A), that a restriction must be continued in order to ensure public safety at the airport is—

''(i) 15 days for a nonhub airport (as defined in section 41714(h) of title 49, United States Code);

''(ii) 30 days for a small hub airport (as defined in such section);

''(iii) 60 days for a medium hub airport (as defined in such section); and

''(iv) 120 days for an airport that had at least 1 percent of the total annual enplanements in the United States for the most recent calendar year for which data is available.''

AIRPORT SECURITY AWARENESS PROGRAMS

Pub. L. 107–71, title I, §106(e), Nov. 19, 2001, 115 Stat. 610, provided that: ''The Under Secretary of Transportation for Security [now Administrator of the Transportation Security Administration] shall require scheduled passenger air carriers, and airports in the United States described in section 44903(c) [of title 49] to develop security awareness programs for airport employees, ground crews, gate, ticket, and curbside agents of the air carriers, and other individuals employed at such airports.''

AIRLINE COMPUTER RESERVATION SYSTEMS

Pub. L. 107–71, title I, §117, Nov. 19, 2001, 115 Stat. 624, provided that: ''In order to ensure that all airline computer reservation systems maintained by United States air carriers are secure from unauthorized access by persons seeking information on reservations, passenger manifests, or other nonpublic information, the Secretary of Transportation shall require all such air carriers to utilize to the maximum extent practicable the best technology available to secure their computer reservation system against such unauthorized access.''

AUTHORIZATION OF FUNDS FOR REIMBURSEMENT OF AIRPORTS FOR SECURITY MANDATES

Pub. L. 107–71, title I, §121, Nov. 19, 2001, 115 Stat. 630, provided that:

''(a) AIRPORT SECURITY.—There is authorized to be appropriated to the Secretary of Transportation for fiscal years 2002 and 2003 a total of $1,500,000,000 to reimburse airport operators, on-airport parking lots, and vendors of on-airfield direct services to air carriers for direct costs incurred by such operators to comply with new, additional, or revised security requirements imposed on such operators by the Federal Aviation Administration or Transportation Security Administration on or after September 11, 2001. Such sums shall remain available until expended.

''(b) DOCUMENTATION OF COSTS; AUDIT.—The Secretary may not reimburse an airport operator, on-airport parking lot, or vendor of on-airfield direct services to air carriers under this section for any cost for which the airport operator, on-airport parking lot, or vendor of on-airfield direct services does not demonstrate to the satisfaction of the Secretary, using sworn financial statements or other appropriate data, that—

''(1) the cost is eligible for reimbursement under subsection (a); and

''(2) the cost was incurred by the airport operator, on-airport parking lot, or vendor of on-airfield direct services to air carriers.

The Inspector General of the Department of Transportation and the Comptroller General of the United States may audit such statements and may request any other information necessary to conduct such an audit.

''(c) CLAIM PROCEDURE.—Within 30 days after the date of enactment of this Act [Nov. 19, 2001], the Secretary, after consultation with airport operators, on-airport parking lots, and vendors of on-airfield direct services to air carriers, shall publish in the Federal Register the procedures for filing claims for reimbursement under this section of eligible costs incurred by airport operators.''

FLIGHT DECK SECURITY

Pub. L. 107–71, title I, §128, Nov. 19, 2001, 115 Stat. 633, which authorized the pilot of a passenger aircraft to carry a firearm into the cockpit if approved by the Under Secretary of Transportation for Security and the air carrier, if the firearm is approved by the Under Secretary, and if the pilot has received proper training, was repealed by Pub. L. 107–296, title XIV, §1402(b)(2), Nov. 25, 2002, 116 Stat. 2305.

CHARTER AIR CARRIERS

Pub. L. 107–71, title I, §132(a), Nov. 19, 2001, 115 Stat. 635, which provided that within 90 days after Nov. 19, 2001, the Under Secretary of Transportation for Security was to implement an aviation security program for charter air carriers with a maximum certificated takeoff weight of 12,500 pounds or more, was repealed by Pub. L. 108–176, title VI, §606(b), Dec. 12, 2003, 117 Stat. 2568.

PHYSICAL SECURITY FOR ATC FACILITIES

Pub. L. 106–528, §5, Nov. 22, 2000, 114 Stat. 2521, provided that:

''(a) IN GENERAL.—In order to ensure physical security at Federal Aviation Administration staffed facilities that house air traffic control systems, the Administrator of the Federal Aviation Administration shall act immediately to—

''(1) correct physical security weaknesses at air traffic control facilities so the facilities can be granted physical security accreditation not later than April 30, 2004; and

''(2) ensure that follow-up inspections are conducted, deficiencies are promptly corrected, and accreditation is kept current for all air traffic control facilities.

''(b) REPORTS.—Not later than April 30, 2001, and annually thereafter through April 30, 2004, the Administrator shall transmit to the Committee on Commerce, Science, and Transportation of the Senate and the Committee on Transportation and Infrastructure of the House of Representatives a report on the progress being made in improving the physical security of air traffic control facilities, including the percentage of such facilities that have been granted physical security accreditation.''

DEPUTIZING OF STATE AND LOCAL LAW ENFORCEMENT OFFICERS

Pub. L. 106–181, title V, §512, Apr. 5, 2000, 114 Stat. 142, provided that:

''(a) DEFINITIONS.—In this section, the following definitions apply:

''(1) AIRCRAFT.—The term 'aircraft' has the meaning given that term in section 40102 of title 49, United States Code.

''(2) AIR TRANSPORTATION.—The term 'air transportation' has the meaning given that term in such section.

''(3) PROGRAM.—The term 'program' means the program established under subsection (b)(1)(A).

''(b) ESTABLISHMENT OF A PROGRAM TO DEPUTIZE LOCAL LAW ENFORCEMENT OFFICERS.—

''(1) IN GENERAL.—The Attorney General may—

''(A) establish a program under which the Attorney General may deputize State and local law enforcement officers having jurisdiction over airports and airport authorities as Deputy United States Marshals for the limited purpose of enforcing Federal laws that regulate security on board aircraft, including laws relating to violent, abusive, or disruptive behavior by passengers in air transportation; and

''(B) encourage the participation of law enforcement officers of State and local governments in the program.

''(2) CONSULTATION.—In establishing the program, the Attorney General shall consult with appropriate officials of—

''(A) the United States Government (including the Administrator [of the Federal Aviation Administration] or a designated representative of the Administrator); and

''(B) State and local governments in any geographic area in which the program may operate.

''(3) TRAINING AND BACKGROUND OF LAW ENFORCEMENT OFFICERS.—

''(A) IN GENERAL.—Under the program, to qualify to serve as a Deputy United States Marshal under the program, a State or local law enforcement officer shall—

''(i) meet the minimum background and training requirements for a law enforcement officer under part 107 of title 14, Code of Federal Regulations (or equivalent requirements established by the Attorney General); and

''(ii) receive approval to participate in the program from the State or local law enforcement agency that is the employer of that law enforcement officer.

''(B) TRAINING NOT FEDERAL RESPONSIBILITY.—The United States Government shall not be responsible for providing to a State or local law enforcement officer the training required to meet the training requirements under subparagraph (A)(i). Nothing in this subsection may be construed to grant any such law enforcement officer the right to attend any institution of the United States Government established to provide training to law enforcement officers of the United States Government.

''(c) POWERS AND STATUS OF DEPUTIZED LAW ENFORCEMENT OFFICERS.—

''(1) IN GENERAL.—Subject to paragraph (2), a State or local law enforcement officer that is deputized as a Deputy United States Marshal under the program may arrest and apprehend an individual suspected of violating any Federal law described in subsection (b)(1)(A), including any individual who violates a provision subject to a civil penalty under section 46301 of title 49, United States Code, or section 46302, 46303, 46318, 46504, 46505, or 46507 of that title, or who commits an act described in section 46506 of that title.

''(2) LIMITATION.—The powers granted to a State or local law enforcement officer deputized under the program shall be limited to enforcing Federal laws relating to security on board aircraft in flight.

''(3) STATUS.—A State or local law enforcement officer that is deputized as a Deputy United States Marshal under the program shall not—

''(A) be considered to be an employee of the United States Government; or

''(B) receive compensation from the United States Government by reason of service as a Deputy United States Marshal under the program.

''(d) STATUTORY CONSTRUCTION.—Nothing in this section may be construed to—

''(1) grant a State or local law enforcement officer that is deputized under the program the power to enforce any Federal law that is not described in subsection (c); or

''(2) limit the authority that a State or local law enforcement officer may otherwise exercise in the officer's capacity under any other applicable State or Federal law.

''(e) REGULATIONS.—The Attorney General may promulgate such regulations as may be necessary to carry out this section.

''(f) NOTIFICATION OF CONGRESS.—Not later than 90 days after the date of the enactment of this Act [Apr. 5, 2000], the Attorney General shall notify the Committee on Transportation and Infrastructure of the House of Representatives and the Committee on Commerce, Science, and Transportation of the Senate on whether or not the Attorney General intends to establish the program authorized by this section.''

DEVELOPMENT OF AVIATION SECURITY LIAISON AGREEMENT

Pub. L. 104–264, title III, § 309, Oct. 9, 1996, 110 Stat. 3253, provided that: ''The Secretary of Transportation and the Attorney General, acting through the Administrator of the Federal Aviation Administration and the Director of the Federal Bureau of Investigation, shall enter into an interagency agreement providing for the establishment of an aviation security liaison at existing appropriate Federal agencies' field offices in or near cities served by a designated high-risk airport.''

DEFINITIONS OF TERMS IN PUB. L. 107–71

For definitions of terms used in sections 104, 106(b), (e), 117, 121, 128, and 132(a) of Pub. L. 107–71, set out above, see section 133 of Pub. L. 107–71, set out as a note under section 40102 of this title.

§ 44904. Domestic air transportation system security

(a) ASSESSING THREATS.—The Administrator of the Transportation Security Administration and the Director of the Federal Bureau of Investigation jointly shall assess current and potential threats to the domestic air transportation system. The assessment shall include consideration of the extent to which there are individuals with the capability and intent to carry out terrorist or related unlawful acts against that system and the ways in which those individuals might carry out those acts. The Administrator of the Transportation Security Administration and the Director jointly shall decide on and carry out the most effective method for continuous analysis and monitoring of security threats to that system.

(b) ASSESSING SECURITY.—In coordination with the Director, the Administrator of the Transportation Security Administration shall carry out periodic threat and vulnerability assessments on security at each airport that is part of the domestic air transportation system. Each assessment shall include consideration of—

(1) the adequacy of security procedures related to the handling and transportation of checked baggage and cargo;

(2) space requirements for security personnel and equipment;

(3) separation of screened and unscreened passengers, baggage, and cargo;

(4) separation of the controlled and uncontrolled areas of airport facilities; and

(5) coordination of the activities of security personnel of the Transportation Security Administration, the United States Customs Service, the Immigration and Naturalization Service, and air carriers, and of other law enforcement personnel.

(c) MODAL SECURITY PLAN FOR AVIATION.—In addition to the requirements set forth in subparagraphs (B) through (F) of section 114(s)(3), the modal security plan for aviation prepared under section 114(s) shall—

(1) establish a damage mitigation and recovery plan for the aviation system in the event of a terrorist attack; and

(2) include a threat matrix document that outlines each threat to the United States civil aviation system and the corresponding layers of security in place to address such threat.

(d) OPERATIONAL CRITERIA.—The Administrator of the Transportation Security Administration shall issue operational criteria to protect airport infrastructure and operations against the threats identified in the plans prepared under section 114(s)(1) and shall approve best practices guidelines for airport assets.

(e) IMPROVING SECURITY.—The Administrator of the Transportation Security Administration