

§ 556. Incidental transfers

The Director of the Office of Management and Budget, in consultation with the Secretary, is authorized and directed to make such additional incidental dispositions of personnel, assets, and liabilities held, used, arising from, available, or to be made available, in connection with the functions transferred by this chapter, as the Director may determine necessary to accomplish the purposes of this chapter.

(Pub. L. 107–296, title XV, § 1516, Nov. 25, 2002, 116 Stat. 2311.)

Editorial Notes**REFERENCES IN TEXT**

This chapter, referred to in text, was in the original “this Act”, meaning Pub. L. 107–296, Nov. 25, 2002, 116 Stat. 2135, known as the Homeland Security Act of 2002, which is classified principally to this chapter. For complete classification of this Act to the Code, see Short Title note set out under section 101 of this title and Tables.

§ 557. Reference

With respect to any function transferred by or under this chapter (including under a reorganization plan that becomes effective under section 542 of this title) and exercised on or after the effective date of this chapter, reference in any other Federal law to any department, commission, or agency or any officer or office the functions of which are so transferred shall be deemed to refer to the Secretary, other official, or component of the Department to which such function is so transferred.

(Pub. L. 107–296, title XV, § 1517, Nov. 25, 2002, 116 Stat. 2311.)

Editorial Notes**REFERENCES IN TEXT**

This chapter, referred to in text, was in the original “this Act”, meaning Pub. L. 107–296, Nov. 25, 2002, 116 Stat. 2135, known as the Homeland Security Act of 2002, which is classified principally to this chapter. For complete classification of this Act to the Code, see Short Title note set out under section 101 of this title and Tables.

The effective date of this chapter, referred to in text, is 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 this title.

SUBCHAPTER XII—TRANSPORTATION SECURITY

PART A—GENERAL PROVISIONS

§ 561. Definitions

In this subchapter:

(1) Administration

The term “Administration” means the Transportation Security Administration.

(2) Administrator

The term “Administrator” means the Administrator of the Transportation Security Administration.

(3) Plan

The term “Plan” means the strategic 5-year technology investment plan developed by the Administrator under section 563 of this title.

(4) Security-related technology

The term “security-related technology” means any technology that assists the Administration in the prevention of, or defense against, threats to United States transportation systems, including threats to people, property, and information.

(Pub. L. 107–296, title XVI, § 1601, as added Pub. L. 113–245, § 3(a), Dec. 18, 2014, 128 Stat. 2871.)

Editorial Notes**PRIOR PROVISIONS**

A prior section 1601 of Pub. L. 107–296, title XVI, Nov. 25, 2002, 116 Stat. 2312, amended sections 114 and 40119 of Title 49, Transportation, see section 3(c) of Pub. L. 113–245, set out as a note below.

Statutory Notes and Related Subsidiaries**FINDINGS**

Pub. L. 113–245, § 2, Dec. 18, 2014, 128 Stat. 2871, provided that: “Congress finds the following:

“(1) The Transportation Security Administration has not consistently implemented Department of Homeland Security policies and Government best practices for acquisition and procurement.

“(2) The Transportation Security Administration has only recently developed a multiyear technology investment plan, and has underutilized innovation opportunities within the private sector, including from small businesses.

“(3) The Transportation Security Administration has faced challenges in meeting key performance requirements for several major acquisitions and procurements, resulting in reduced security effectiveness and wasted expenditures.”

PRIOR AMENDMENTS NOT AFFECTED

Pub. L. 113–245, § 3(c), Dec. 18, 2014, 128 Stat. 2877, provided that: “Nothing in this section [enacting this subchapter] may be construed to affect any amendment made by title XVI of the Homeland Security Act of 2002 [title XVI of Pub. L. 107–296, amending sections 114, 40119, 44935 and 46301 of Title 49, Transportation] as in effect before the date of enactment of this Act [Dec. 18, 2014].”

PART B—TRANSPORTATION SECURITY ADMINISTRATION ACQUISITION IMPROVEMENTS

§ 563. 5-year technology investment plan**(a) In general**

The Administrator shall—

(1) not later than 180 days after December 18, 2014, develop and submit to Congress a strategic 5-year technology investment plan, that may include a classified addendum to report sensitive transportation security risks, technology vulnerabilities, or other sensitive security information; and

(2) to the extent possible, publish the Plan in an unclassified format in the public domain.

(b) Consultation

The Administrator shall develop the Plan in consultation with—

(1) the Under Secretary for Management;

(2) the Under Secretary for Science and Technology;

(3) the Chief Information Officer; and

(4) the aviation industry stakeholder advisory committee established by the Administrator.

(c) Approval

The Administrator may not publish the Plan under subsection (a)(2) until it has been approved by the Secretary.

(d) Contents of Plan

The Plan shall include—

(1) an analysis of transportation security risks and the associated capability gaps that would be best addressed by security-related technology, including consideration of the most recent quadrennial homeland security review under section 347 of this title;

(2) a set of security-related technology acquisition needs that—

(A) is prioritized based on risk and associated capability gaps identified under paragraph (1); and

(B) includes planned technology programs and projects with defined objectives, goals, timelines, and measures;

(3) an analysis of current and forecast trends in domestic and international passenger travel;

(4) an identification of currently deployed security-related technologies that are at or near the end of their lifecycles;

(5) an identification of test, evaluation, modeling, and simulation capabilities, including target methodologies, rationales, and timelines necessary to support the acquisition of the security-related technologies expected to meet the needs under paragraph (2);

(6) an identification of opportunities for public-private partnerships, small and disadvantaged company participation, intragovernment collaboration, university centers of excellence, and national laboratory technology transfer;

(7) an identification of the Administration's acquisition workforce needs for the management of planned security-related technology acquisitions, including consideration of leveraging acquisition expertise of other Federal agencies;

(8) an identification of the security resources, including information security resources, that will be required to protect security-related technology from physical or cyber theft, diversion, sabotage, or attack;

(9) an identification of initiatives to streamline the Administration's acquisition process and provide greater predictability and clarity to small, medium, and large businesses, including the timeline for testing and evaluation;

(10) an assessment of the impact to commercial aviation passengers;

(11) a strategy for consulting airport management, air carrier representatives, and Federal security directors whenever an acquisition will lead to the removal of equipment at airports, and how the strategy for consulting with such officials of the relevant airports will address potential negative impacts on commercial passengers or airport operations; and

(12) in consultation with the National Institutes of Standards and Technology, an identification of security-related technology interface standards, in existence or if implemented, that could promote more interoperable passenger, baggage, and cargo screening systems.

(e) Leveraging the private sector

To the extent possible, and in a manner that is consistent with fair and equitable practices, the Plan shall—

(1) leverage emerging technology trends and research and development investment trends within the public and private sectors;

(2) incorporate private sector input, including from the aviation industry stakeholder advisory committee established by the Administrator, through requests for information, industry days, and other innovative means consistent with the Federal Acquisition Regulation; and

(3) in consultation with the Under Secretary for Science and Technology, identify technologies in existence or in development that, with or without adaptation, are expected to be suitable to meeting mission needs.

(f) Disclosure

The Administrator shall include with the Plan a list of nongovernment persons that contributed to the writing of the Plan.

(g) Update and report

The Administrator shall, in collaboration with relevant industry and government stakeholders, annually submit to Congress in an appendix to the budget request and publish in an unclassified format in the public domain—

(1) an update of the Plan;

(2) a report on the extent to which each security-related technology acquired by the Administration since the last issuance or update of the Plan is consistent with the planned technology programs and projects identified under subsection (d)(2) for that security-related technology; and

(3) information about acquisitions completed during the fiscal year preceding the fiscal year during which the report is submitted.

(h) Additional update requirements

Updates and reports under subsection (g) shall—

(1) be prepared in consultation with—

(A) the persons described in subsection (b); and

(B) the Surface Transportation Security Advisory Committee established under section 204 of this title; and

(2) include—

(A) information relating to technology investments by the Transportation Security Administration and the private sector that the Department supports with research, development, testing, and evaluation for aviation, including air cargo, and surface transportation security;

(B) information about acquisitions completed during the fiscal year preceding the fiscal year during which the report is submitted;

(C) information relating to equipment of the Transportation Security Administration that is in operation after the end of the lifecycle of the equipment specified by the manufacturer of the equipment; and

(D) to the extent practicable, a classified addendum to report sensitive transportation

security risks and associated capability gaps that would be best addressed by security-related technology described in subparagraph (A).

(i) Notice of covered changes to plan

(1) Notice required

The Administrator shall submit to the Committee on Commerce, Science, and Transportation of the Senate and the Committee on Homeland Security of the House of Representatives notice of any covered change to the Plan not later than 90 days after the date that the covered change is made.

(2) Definition of covered change

In this subsection, the term “covered change” means—

(A) an increase or decrease in the dollar amount allocated to the procurement of a technology; or

(B) an increase or decrease in the number of a technology.

(Pub. L. 107-296, title XVI, §1611, as added Pub. L. 113-245, §3(a), Dec. 18, 2014, 128 Stat. 2872; amended Pub. L. 115-254, div. K, title I, §1917, Oct. 5, 2018, 132 Stat. 3557.)

Editorial Notes

AMENDMENTS

2018—Subsec. (g). Pub. L. 115-254, §1917(1)(A), substituted “The Administrator shall, in collaboration with relevant industry and government stakeholders, annually submit to Congress in an appendix to the budget request and publish in an unclassified format in the public domain—” for “Beginning 2 years after the date the Plan is submitted to Congress under subsection (a), and biennially thereafter, the Administrator shall submit to Congress—” in introductory provisions.

Subsec. (g)(3). Pub. L. 115-254, §1917(1)(B)–(D), added par. (3).

Subsecs. (h), (i). Pub. L. 115-254, §1917(2), added subsecs. (h) and (i).

§ 563a. Acquisition justification and reports

(a) Acquisition justification

Before the Administration implements any security-related technology acquisition, the Administrator, in accordance with the Department’s policies and directives, shall determine whether the acquisition is justified by conducting an analysis that includes—

(1) an identification of the scenarios and level of risk to transportation security from those scenarios that would be addressed by the security-related technology acquisition;

(2) an assessment of how the proposed acquisition aligns to the Plan;

(3) a comparison of the total expected lifecycle cost against the total expected quantitative and qualitative benefits to transportation security;

(4) an analysis of alternative security solutions, including policy or procedure solutions, to determine if the proposed security-related technology acquisition is the most effective and cost-efficient solution based on cost-benefit considerations;

(5) an assessment of the potential privacy and civil liberties implications of the proposed

acquisition that includes, to the extent practicable, consultation with organizations that advocate for the protection of privacy and civil liberties;

(6) a determination that the proposed acquisition is consistent with fair information practice principles issued by the Privacy Officer of the Department;

(7) confirmation that there are no significant risks to human health or safety posed by the proposed acquisition; and

(8) an estimate of the benefits to commercial aviation passengers.

(b) Reports and certification to Congress

(1) In general

Not later than the end of the 30-day period preceding the award by the Administration of a contract for any security-related technology acquisition exceeding \$30,000,000, the Administrator shall submit to the Committee on Commerce, Science, and Transportation of the Senate and the Committee on Homeland Security of the House of Representatives—

(A) the results of the comprehensive acquisition justification under subsection (a); and

(B) a certification by the Administrator that the benefits to transportation security justify the contract cost.

(2) Extension due to imminent terrorist threat

If there is a known or suspected imminent threat to transportation security, the Administrator—

(A) may reduce the 30-day period under paragraph (1) to 5 days to rapidly respond to the threat; and

(B) shall immediately notify the Committee on Commerce, Science, and Transportation of the Senate and the Committee on Homeland Security of the House of Representatives of the known or suspected imminent threat.

(Pub. L. 107-296, title XVI, §1612, as added Pub. L. 113-245, §3(a), Dec. 18, 2014, 128 Stat. 2873.)

§ 563b. Acquisition baseline establishment and reports

(a) Baseline requirements

(1) In general

Before the Administration implements any security-related technology acquisition, the appropriate acquisition official of the Department shall establish and document a set of formal baseline requirements.

(2) Contents

The baseline requirements under paragraph

(1) shall—

(A) include the estimated costs (including lifecycle costs), schedule, and performance milestones for the planned duration of the acquisition;

(B) identify the acquisition risks and a plan for mitigating those risks; and

(C) assess the personnel necessary to manage the acquisition process, manage the ongoing program, and support training and other operations as necessary.

(3) Feasibility

In establishing the performance milestones under paragraph (2)(A), the appropriate acqui-

sition official of the Department, to the extent possible and in consultation with the Under Secretary for Science and Technology, shall ensure that achieving those milestones is technologically feasible.

(4) Test and evaluation plan

The Administrator, in consultation with the Under Secretary for Science and Technology, shall develop a test and evaluation plan that describes—

(A) the activities that are expected to be required to assess acquired technologies against the performance milestones established under paragraph (2)(A);

(B) the necessary and cost-effective combination of laboratory testing, field testing, modeling, simulation, and supporting analysis to ensure that such technologies meet the Administration's mission needs;

(C) an efficient planning schedule to ensure that test and evaluation activities are completed without undue delay; and

(D) if commercial aviation passengers are expected to interact with the security-related technology, methods that could be used to measure passenger acceptance of and familiarization with the security-related technology.

(5) Verification and validation

The appropriate acquisition official of the Department—

(A) subject to subparagraph (B), shall utilize independent reviewers to verify and validate the performance milestones and cost estimates developed under paragraph (2) for a security-related technology that pursuant to section 563(d)(2) of this title has been identified as a high priority need in the most recent Plan; and

(B) shall ensure that the use of independent reviewers does not unduly delay the schedule of any acquisition.

(6) Streamlining access for interested vendors

The Administrator shall establish a streamlined process for an interested vendor of a security-related technology to request and receive appropriate access to the baseline requirements and test and evaluation plans that are necessary for the vendor to participate in the acquisitions process for that technology.

(b) Review of baseline requirements and deviation; report to Congress

(1) Review

(A) In general

The appropriate acquisition official of the Department shall review and assess each implemented acquisition to determine if the acquisition is meeting the baseline requirements established under subsection (a).

(B) Test and evaluation assessment

The review shall include an assessment of whether—

(i) the planned testing and evaluation activities have been completed; and

(ii) the results of that testing and evaluation demonstrate that the performance milestones are technologically feasible.

(2) Report

Not later than 30 days after making a finding described in clause (i), (ii), or (iii) of subparagraph (A), the Administrator 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 includes—

(A) the results of any assessment that finds that—

(i) the actual or planned costs exceed the baseline costs by more than 10 percent;

(ii) the actual or planned schedule for delivery has been delayed by more than 180 days; or

(iii) there is a failure to meet any performance milestone that directly impacts security effectiveness;

(B) the cause for such excessive costs, delay, or failure; and

(C) a plan for corrective action.

(Pub. L. 107–296, title XVI, §1613, as added Pub. L. 113–245, §3(a), Dec. 18, 2014, 128 Stat. 2874.)

§ 563c. Inventory utilization

(a) In general

Before the procurement of additional quantities of equipment to fulfill a mission need, the Administrator, to the extent practicable, shall utilize any existing units in the Administration's inventory to meet that need.

(b) Tracking of inventory

(1) In general

The Administrator shall establish a process for tracking—

(A) the location of security-related equipment in the inventory under subsection (a);

(B) the utilization status of security-related technology in the inventory under subsection (a); and

(C) the quantity of security-related equipment in the inventory under subsection (a).

(2) Internal controls

The Administrator shall implement internal controls to ensure up-to-date accurate data on security-related technology owned, deployed, and in use.

(c) Logistics management

(1) In general

The Administrator shall establish logistics principles for managing inventory in an effective and efficient manner.

(2) Limitation on just-in-time logistics

The Administrator may not use just-in-time logistics if doing so—

(A) would inhibit necessary planning for large-scale delivery of equipment to airports or other facilities; or

(B) would unduly diminish surge capacity for response to a terrorist threat.

(Pub. L. 107–296, title XVI, §1614, as added Pub. L. 113–245, §3(a), Dec. 18, 2014, 128 Stat. 2876.)

§ 563d. Small business contracting goals

Not later than 90 days after December 18, 2014, and annually thereafter, the Administrator

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 includes—

(1) the Administration's performance record with respect to meeting its published small-business contracting goals during the preceding fiscal year;

(2) if the goals described in paragraph (1) were not met or the Administration's performance was below the published small-business contracting goals of the Department—

(A) a list of challenges, including deviations from the Administration's subcontracting plans, and factors that contributed to the level of performance during the preceding fiscal year;

(B) an action plan, with benchmarks, for addressing each of the challenges identified in subparagraph (A) that—

(i) is prepared after consultation with the Secretary of Defense and the heads of Federal departments and agencies that achieved their published goals for prime contracting with small and minority-owned businesses, including small and disadvantaged businesses, in prior fiscal years; and

(ii) identifies policies and procedures that could be incorporated by the Administration in furtherance of achieving the Administration's published goal for such contracting; and

(3) a status report on the implementation of the action plan that was developed in the preceding fiscal year in accordance with paragraph (2)(B), if such a plan was required.

(Pub. L. 107-296, title XVI, §1615, as added Pub. L. 113-245, §3(a), Dec. 18, 2014, 128 Stat. 2876.)

§ 563e. Consistency with the Federal Acquisition Regulation and departmental policies and directives

The Administrator shall execute the responsibilities set forth in this part in a manner consistent with, and not duplicative of, the Federal Acquisition Regulation and the Department's policies and directives.

(Pub. L. 107-296, title XVI, §1616, as added Pub. L. 113-245, §3(a), Dec. 18, 2014, 128 Stat. 2877.)

§ 563f. Diversified security technology industry marketplace

(a) In general

Not later than 120 days after October 5, 2018, the Administrator shall develop and submit to the Committee on Commerce, Science, and Transportation of the Senate and the Committee on Homeland Security of the House of Representatives a strategy to promote a diverse security technology industry marketplace upon which the Administrator can rely to acquire advanced transportation security technologies or capabilities, including by increased participation of small business innovators.

(b) Contents

The strategy required under subsection (a) shall include the following:

(1) Information on how existing Administration solicitation, testing, evaluation, piloting, acquisition, and procurement processes impact the Administrator's ability to acquire from the security technology industry marketplace, including small business innovators that have not previously provided technology to the Administration, innovative technologies or capabilities with the potential to enhance transportation security.

(2) Specific actions that the Administrator will take, including modifications to the processes described in paragraph (1), to foster diversification within the security technology industry marketplace.

(3) Projected timelines for implementing the actions described in paragraph (2).

(4) Plans for how the Administrator could, to the extent practicable, assist a small business innovator periodically during such processes, including when such an innovator lacks adequate resources to participate in such processes, to facilitate an advanced transportation security technology or capability being developed and acquired by the Administrator.

(5) An assessment of the feasibility of partnering with an organization described in section 501(c)(3) of title 26 and exempt from tax under section 501(a) of title 26 to provide venture capital to businesses, particularly small business innovators, for commercialization of innovative transportation security technologies that are expected to be ready for commercialization in the near term and within 36 months.

(c) Feasibility assessment

In conducting the feasibility assessment under subsection (b)(5), the Administrator shall consider the following:

(1) Establishing an organization described in section 501(c)(3) of title 26 and exempt from tax under section 501(a) of title 26 as a venture capital partnership between the private sector and the intelligence community to help businesses, particularly small business innovators, commercialize innovative security-related technologies.

(2) Enhanced engagement through the Science and Technology Directorate of the Department of Homeland Security.

(d) Rule of construction

Nothing in this section may be construed as requiring changes to the Transportation Security Administration standards for security technology.

(e) Definitions

In this section:

(1) Intelligence community

The term "intelligence community" has the meaning given the term in section 3003 of title 50.

(2) Small business concern

The term "small business concern" has the meaning described under section 632 of title 15.

(3) Small business innovator

The term "small business innovator" means a small business concern that has an advanced

transportation security technology or capability.

(Pub. L. 107-296, title XVI, §1617, as added Pub. L. 115-254, div. K, title I, §1913(a), Oct. 5, 2018, 132 Stat. 3554.)

PART C—MAINTENANCE OF SECURITY-RELATED TECHNOLOGY

§ 565. Maintenance validation and oversight

(a) In general

Not later than 180 days after October 5, 2018, the Administrator shall develop and implement a preventive maintenance validation process for security-related technology deployed to airports.

(b) Maintenance by Administration personnel at airports

For maintenance to be carried out by Administration personnel at airports, the process referred to in subsection (a) shall include the following:

- (1) Guidance to Administration personnel at airports specifying how to conduct and document preventive maintenance actions.
- (2) Mechanisms for the Administrator to verify compliance with the guidance issued pursuant to paragraph (1).

(c) Maintenance by contractors at airports

For maintenance to be carried by a contractor at airports, the process referred to in subsection (a) shall require the following:

- (1) Provision of monthly preventative maintenance schedules to appropriate Administration personnel at each airport that includes information on each action to be completed by contractor.¹
- (2) Notification to appropriate Administration personnel at each airport when maintenance action is completed by a contractor.
- (3) A process for independent validation by a third party of contractor maintenance.

(d) Penalties for noncompliance

The Administrator shall require maintenance for any contracts entered into 60 days after October 5, 2018, or later for security-related technology deployed to airports to include penalties for noncompliance when it is determined that either preventive or corrective maintenance has not been completed according to contractual requirements and manufacturers' specifications.

(Pub. L. 107-296, title XVI, §1621, as added Pub. L. 115-254, div. K, title I, §1918(a), Oct. 5, 2018, 132 Stat. 3558.)

SUBCHAPTER XIII—EMERGENCY COMMUNICATIONS

Editorial Notes

CODIFICATION

This subchapter is comprised of title XVIII of Pub. L. 107-296, as added by Pub. L. 109-295, title VI, §671(b), Oct. 4, 2006, 120 Stat. 1433. Another title XVIII of Pub. L. 107-296 was renumbered title XIX and is classified to subchapter XIV (§591 et seq.) of this chapter.

¹ So in original. Probably should be preceded by "a".

§ 571. Emergency Communications Division

(a) In general

There is established in the Department an Emergency Communications Division. The Division shall be located in the Cybersecurity and Infrastructure Security Agency.

(b) Executive Assistant Director

The head of the Division shall be the Executive Assistant Director for Emergency Communications (in this section referred to as the "Executive Assistant Director"). The Executive Assistant Director shall report to the Director of the Cybersecurity and Infrastructure Security Agency. All decisions of the Executive Assistant Director that entail the exercise of significant authority shall be subject to the approval of the Director of the Cybersecurity and Infrastructure Security Agency.

(c) Responsibilities

The Executive Assistant Director shall—

- (1) assist the Secretary in developing and implementing the program described in section 194(a)(1) of this title, except as provided in section 195 of this title;
- (2) administer the Department's responsibilities and authorities relating to the SAFECOM Program, excluding elements related to research, development, testing, and evaluation and standards;
- (3) administer the Department's responsibilities and authorities relating to the Integrated Wireless Network program;
- (4) conduct extensive, nationwide outreach to support and promote the ability of emergency response providers and relevant government officials to continue to communicate in the event of natural disasters, acts of terrorism, and other man-made disasters;
- (5) conduct extensive, nationwide outreach and foster the development of interoperable emergency communications capabilities by State, regional, local, and tribal governments and public safety agencies, and by regional consortia thereof;
- (6) provide technical assistance to State, regional, local, and tribal government officials with respect to use of interoperable emergency communications capabilities;
- (7) coordinate with the Regional Administrators regarding the activities of Regional Emergency Communications Coordination Working Groups under section 575 of this title;
- (8) promote the development of standard operating procedures and best practices with respect to use of interoperable emergency communications capabilities for incident response, and facilitate the sharing of information on such best practices for achieving, maintaining, and enhancing interoperable emergency communications capabilities for such response;
- (9) coordinate, in cooperation with the National Communications System, the establishment of a national response capability with initial and ongoing planning, implementation, and training for the deployment of communications equipment for relevant State, local, and tribal governments and emergency response providers in the event of a catastrophic loss of local and regional emergency communications services;