

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.<sup>1</sup>
- (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.

<sup>1</sup> 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;