

116TH CONGRESS
1ST SESSION

H. R. 3318

To require the Transportation Security Administration to establish a task force to conduct an analysis of emerging and potential future threats to transportation security, and for other purposes.

IN THE HOUSE OF REPRESENTATIVES

JUNE 18, 2019

Mr. JOYCE of Pennsylvania (for himself and Mr. ROGERS of Alabama) introduced the following bill; which was referred to the Committee on Homeland Security

A BILL

To require the Transportation Security Administration to establish a task force to conduct an analysis of emerging and potential future threats to transportation security, and for other purposes.

1 *Be it enacted by the Senate and House of Representa-*
2 *tives of the United States of America in Congress assembled,*

3 **SECTION 1. SHORT TITLE.**

4 This Act may be cited as the “Emerging Transpor-
5 tation Security Threats Act of 2019”.

6 **SEC. 2. EMERGING AND FUTURE THREATS TASK FORCE.**

7 (a) IN GENERAL.—Not later than 90 days after the
8 date of the enactment of this Act, the Administrator of

1 the Transportation Security Administration, in consulta-
2 tion with the Director of National Intelligence and the in-
3 telligence community (as such term is defined in section
4 3(4) of the National Security Act of 1947 (50 U.S.C.
5 3003(4))) and the heads of other Federal agencies, as de-
6 termined appropriate by the Administrator, shall establish
7 a task force to conduct an analysis of emerging and poten-
8 tial future threats to transportation security.

9 (b) ELEMENTS.—The analysis required under sub-
10 section (a) shall include emerging and potential future
11 threats posed by the following:

12 (1) Evolving tactics by terrorist organizations
13 that may pose a catastrophic risk to an aviation or
14 surface transportation entity.

15 (2) Explosive and explosive devices or attacks
16 involving the use of explosives that may cause cata-
17 strophic damage to an aviation or surface transpor-
18 tation system.

19 (3) Chemical or biological agents being released
20 in either aviation or surface transportation systems.

21 (4) Cyberthreat actors seeking to undermine
22 confidence in transportation systems or cause service
23 disruptions that jeopardize transportation security.

24 (5) Unmanned aerial systems with the capa-
25 bility of inflicting harm on transportation targets.

1 (6) Individuals or groups seeking to attack soft
2 targets, public areas, or crowded spaces of transpor-
3 tation systems.

4 (7) Inconsistent or inadequate security screen-
5 ing protocols at last point of departure airports with
6 direct flights to the United States.

7 (8) Information sharing challenges within the
8 Federal Government and among partner govern-
9 ments.

10 (9) Information sharing challenges between the
11 Administration or other relevant Federal agencies
12 and transportation stakeholders, including air car-
13 riers, airport operators, surface transportation oper-
14 ators, and State and local law enforcement.

15 (10) Growth in passenger volume in both the
16 aviation and surface transportation sectors.

17 (c) MITIGATION.—Not later than 120 days after the
18 completion of the analysis required under subsection (a),
19 the Administrator of the Transportation Security Admin-
20 istration shall develop, as appropriate, a threat mitigation
21 strategy for each of the threats examined in such analysis,
22 and—

23 (1) assign appropriate resources of the Admin-
24 istration to address such threats, based on cal-
25 culated risk; or

1 (2) provide recommendations through the De-
2 partment of Homeland Security to the appropriate
3 Federal department or agency responsible for ad-
4 dressing such threats.

5 (d) **STAKEHOLDER ENGAGEMENT.**—When carrying
6 out the analysis required under subsection (a), the Admin-
7 istrator of the Transportation Security Administration
8 shall engage transportation stakeholders referred to in
9 subsection (b)(9) and account for security concerns of
10 transportation operators by—

11 (1) convening not fewer than three industry day
12 events for such transportation stakeholders to hear
13 from relevant public and private sector security part-
14 ners and provide feedback on threats such transpor-
15 tation stakeholders identify as emerging;

16 (2) developing strategies to solicit feedback on
17 a consistent basis from such transportation stake-
18 holders across all modes of transportation and pro-
19 viding consistent responses to stakeholder concerns;

20 (3) improving the quality and relevancy of in-
21 formation sharing products disseminated by the Ad-
22 ministration to such transportation stakeholders, in-
23 cluding classified information sharing products;

24 (4) coordinating security incident response and
25 communications drills, including tabletop exercises,

1 to improve incident preparedness and response capa-
2 bilities across transportation modes and among
3 transportation systems;

4 (5) encouraging regular communication between
5 Federal Security Directors, Field Intelligence Offi-
6 cers, Federal Air Marshal Special Agents in Charge,
7 and such transportation stakeholders;

8 (6) establishing regular opportunities for senior
9 Administration leadership to engage with such trans-
10 portation stakeholders regarding changes in the
11 threat environment and how the Administration can
12 offer security support to address such changes; and

13 (7) briefing the Aviation Security Advisory
14 Committee and the Surface Transportation Security
15 Advisory Committee on the efforts of the task force
16 established pursuant to subsection (a).

17 (e) BRIEFING TO CONGRESS.—The Administrator of
18 the Transportation Security Administration shall brief the
19 Committee on Homeland Security of the House of Rep-
20 resentatives and the Committee on Commerce, Science,
21 and Transportation of the Senate on the results of the
22 analysis required under subsection (a) and relevant miti-
23 gation strategies developed in accordance with subsection
24 (c).

○