

116TH CONGRESS
1ST SESSION

H. R. 3469

IN THE SENATE OF THE UNITED STATES

DECEMBER 10, 2019

Received; read twice and referred to the Committee on Commerce, Science,
and Transportation

AN ACT

To direct the Transportation Security Administration to
carry out covert testing and risk mitigation improvement
of aviation security operations, 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,*

1 **SECTION 1. SHORT TITLE.**

2 This Act may be cited as the “Covert Testing and
3 Risk Mitigation Improvement Act of 2019”.

4 **SEC. 2. TSA COVERT TESTING AND RISK MITIGATION IM-**
5 **PROVEMENT.**

6 (a) IN GENERAL.—Not later than 180 days after the
7 date of the enactment of this Act and annually thereafter,
8 the Administrator of the Transportation Security Admin-
9 istration shall implement the following:

10 (1) A system for conducting risk-informed
11 headquarters-based covert tests of aviation security
12 operations, including relating to airport passenger
13 and baggage security screening operations, that can
14 yield statistically valid data that can be used to iden-
15 tify and assess the nature and extent of
16 vulnerabilities to such operations that are not miti-
17 gated by current security practices. The Adminis-
18 trator shall execute annually not fewer than three
19 risk-informed covert testing projects designed to
20 identify systemic vulnerabilities in the transportation
21 security system, and shall document the assumptions
22 and rationale guiding the selection of such projects.

23 (2) A long-term headquarters-based covert test-
24 ing program, employing static but risk-informed
25 threat vectors, designed to assess changes in overall
26 screening effectiveness.

1 (b) MITIGATION.—

2 (1) IN GENERAL.—The Administrator of the
3 Transportation Security Administration shall estab-
4 lish a system to address and mitigate the
5 vulnerabilities identified and assessed pursuant to
6 the testing conducted under subsection (a).

7 (2) ANALYSIS.—Not later than 60 days after
8 the identification of any such vulnerability, the Ad-
9 ministrator shall ensure a vulnerability described in
10 paragraph (1) is analyzed to determine root causes.

11 (3) DETERMINATION.—Not later than 120 days
12 after the identification of any such vulnerability, the
13 Administrator shall make a determination regarding
14 whether or not to mitigate such vulnerability. The
15 Administrator shall prioritize mitigating
16 vulnerabilities based on their ability to reduce risk.
17 If the Administrator determines—

18 (A) to not mitigate such vulnerability, the
19 Administrator shall document the reasons for
20 the decision; or

21 (B) to mitigate such vulnerability, the Ad-
22 ministrator shall establish and document—

23 (i) key milestones appropriate for the
24 level of effort required to so mitigate such
25 vulnerability; and

1 (ii) a date by which measures to so
2 mitigate such vulnerability shall be imple-
3 mented by the Transportation Security Ad-
4 ministration.

5 (4) RETESTING.—Not later than 180 days after
6 the date on which measures to mitigate a vulner-
7 ability are completed by the Transportation Security
8 Administration pursuant to paragraph (3)(B)(ii), the
9 Administrator shall conduct a covert test in accord-
10 ance with subsection (a) of the aviation security op-
11 eration with respect to which such vulnerability was
12 identified to assess the effectiveness of such meas-
13 ures to mitigate such vulnerability.

14 (c) COMPILATION OF LISTS.—

15 (1) IN GENERAL.—Not later than 60 days after
16 completing a covert testing protocol under sub-
17 section (a), the Administrator of the Transportation
18 Security Administration shall compile a list (includ-
19 ing a classified annex if necessary) of the
20 vulnerabilities identified and assessed pursuant to
21 such testing. Each such list shall contain, at a min-
22 imum, the following:

23 (A) A brief description of the nature of
24 each vulnerability so identified and assessed.

1 (B) The date on which each vulnerability
2 was so identified and assessed.

3 (C) Key milestones appropriate for the
4 level of effort required to mitigate each vulner-
5 ability, as well as an indication of whether each
6 such milestone has been met.

7 (D) An indication of whether each vulner-
8 ability has been mitigated or reduced and, if so,
9 the date on which each such vulnerability was
10 so mitigated or reduced.

11 (E) If a vulnerability has not been fully
12 mitigated, the date by which the Administrator
13 shall so mitigate such vulnerability or a deter-
14 mination that it is not possible to fully mitigate
15 such vulnerability.

16 (F) The results of any subsequent covert
17 testing undertaken to assess whether mitigation
18 efforts have eliminated or reduced each vulner-
19 ability.

20 (2) SUBMISSION TO CONGRESS.—The Adminis-
21 trator shall submit to the Committee on Homeland
22 Security of the House of Representatives and the
23 Committee on Commerce, Science, and Transpor-
24 tation of the Senate a comprehensive document
25 tracking the status of the information required

Passed the House of Representatives December 9,
2019.

HR 3469 RFS