AUTHENTICATED
U.S. GOVERNMENT
INFORMATION
GPO

I

116TH CONGRESS
1ST SESSION

H. R. 3469

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

IN THE HOUSE OF REPRESENTATIVES

JUNE 25, 2019

Mr. CUMMINGS (for himself, Mr. THOMPSON of Mississippi, Mrs. CAROLYN B. MALONEY of New York, Ms. NORTON, Mr. CLAY, Mr. LYNCH, Mr. COOPER, Mr. CONNOLLY, Mr. KRISHNAMOORTHI, Mr. RASKIN, Mr. ROUDA, Ms. HILL of California, Ms. WASSERMAN SCHULTZ, Mr. SARBANES, Mr. WELCH, Ms. SPEIER, Ms. KELLY of Illinois, Mr. DESAULNIER, Mrs. LAWRENCE, Ms. PLASKETT, Mr. KHANNA, Mr. GOMEZ, Ms. OCASIO-CORTEZ, Ms. PRESSLEY, and Ms. TLAIB) introduced the following bill; which was referred to the Committee on Homeland Security

---

A BILL

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

Be it enacted by the Senate and House of Representatives of the United States of America in Congress assembled,

SECTION 1. SHORT TITLE.

This Act may be cited as the ''Covert Testing and Risk Mitigation Improvement Act of 2019''.

SEC. 2. TSA COVERT TESTING AND RISK MITIGATION IMPROVEMENT.

(a) IN GENERAL.—Not later than 180 days after the date of the enactment of this Act and annually thereafter, the Administrator of the Transportation Security Administration shall implement the following:

(1) A system for conducting risk-informed headquarters-based covert tests of aviation security operations, including relating to airport passenger and baggage security screening operations, that can yield statistically valid data that can be used to identify and assess the nature and extent of vulnerabilities to such operations that are not mitigated by current security practices. The Administrator shall execute annually not fewer than three risk-informed covert testing projects designed to identify systemic vulnerabilities in the transportation security system, and shall document the assumptions and rationale guiding the selection of such projects.

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

(b) MITIGATION.—

(1) IN GENERAL.—The Administrator of the Transportation Security Administration shall estab-

lish a system to address and mitigate the vulnerabilities identified and assessed pursuant to the testing conducted under subsection (a).

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

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

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

(B) to mitigate such vulnerability, the Administrator shall establish and document—

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

(ii) a date by which measures to so mitigate such vulnerability shall be imple-

mented by the Transportation Security Administration.

(4) RETESTING.—Not later than 180 days after the date on which measures to mitigate a vulnerability are completed by the Transportation Security Administration pursuant to paragraph (3)(B)(ii), the Administrator shall conduct a covert test in accordance with subsection (a) of the aviation security operation with respect to which such vulnerability was identified to assess the effectiveness of such measures to mitigate such vulnerability.

(c) COMPILATION OF LISTS.—

(1) IN GENERAL.—Not later than 60 days after completing a covert testing protocol under subsection (a), the Administrator of the Transportation Security Administration shall compile a list (including a classified annex if necessary) of the vulnerabilities identified and assessed pursuant to such testing. Each such list shall contain, at a minimum, the following:

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

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

(C) Key milestones appropriate for the level of effort required to mitigate each vulnerability, as well as an indication of whether each such milestone has been met.

(D) An indication of whether each vulnerability has been mitigated or reduced and, if so, the date on which each such vulnerability was so mitigated or reduced.

(E) If a vulnerability has not been fully mitigated, the date by which the Administrator shall so mitigate such vulnerability or a determination that it is not possible to fully mitigate such vulnerability.

(F) The results of any subsequent covert testing undertaken to assess whether mitigation efforts have eliminated or reduced each vulnerability.

(2) SUBMISSION TO CONGRESS.—The Administrator shall submit to the Committee on Homeland Security of the House of Representatives and the Committee on Commerce, Science, and Transportation of the Senate a comprehensive document tracking the status of the information required under paragraph (1) together with the Transpor-

tation Security Administration's annual budget request.

(d) GAO REVIEW.—Not later than three years after the date of the enactment of this Act, the Comptroller General of the United States shall review and submit to the Administrator of the Transportation Security Administration and the Committee on Homeland Security of the House of Representatives and the Committee on Commerce, Science, and Transportation of the Senate a report on the effectiveness of the Transportation Security Administration's processes for conducting covert testing projects that yield statistically valid data that can be used to assess the nature and extent of vulnerabilities to aviation security operations that are not effectively mitigated by current security operations.

○