United States Government Accountability Office

Testimony

Before the Committee on Oversight and Reform, House of Representatives

For Release on Delivery
Expected at 10:00 a.m. ET
Tuesday, June 25, 2019

AVIATION SECURITY

TSA Has Taken Steps to Conduct More Risk-Informed Covert Tests and Address Vulnerabilities

Statement of Charles Michael Johnson, Jr.
Managing Director, Homeland Security and Justice Team

Chairman Cummings, Ranking Member Jordan, and Members of the Committee:

Thank you for the opportunity to discuss our work on the Transportation Security Administration's (TSA) covert testing activities related to screening passengers and checked baggage. Threats to commercial aviation persist and continue to evolve. In March 2017, more than 15 years after the terrorist attacks of September 11, 2001, TSA imposed new screening measures to enhance security after intelligence agencies confirmed that terrorist organizations had the capability to plant explosives in personal electronic devices, such as laptops.

To help thwart possible attacks, TSA uses covert testing as a key method to identify possible vulnerabilities in the checkpoint and checked baggage screening systems at TSA-regulated (i.e., commercial) airports across the United States.[1] During covert tests, undercover personnel attempt to pass threat items (i.e., guns, simulated improvised explosive devices, etc.) through checkpoint and checked baggage screening equipment undetected.[2] TSA's covert tests are intended to help officials identify vulnerabilities and then address or mitigate them through various means, such as by conducting additional training, revising screening procedures, or adopting new ones.

Within TSA, two offices carry out covert tests of checkpoint and checked baggage screening operations at airports: Inspection and Security Operations. Inspection's tests identify vulnerabilities related to any aspect of TSA's checkpoint and checked baggage screening systems, to include screening procedures and whether the system is vulnerable to threats identified in intelligence reporting.[3] Security Operations' tests focus entirely on Transportation Security Officers' (TSO) performance against standard operating procedures for checkpoint and checked baggage

[1]TSA screening vulnerabilities refer to failures by the people, processes, or equipment involved in aviation security screening to detect specific threats.

[2]The U.S. Bomb Data Center defines the term "improvised explosive device" as a device placed or fabricated in an unconventional manner incorporating destructive, lethal, noxious, pyrotechnic, or incendiary chemicals and designed to destroy, incapacitate, harass, or distract.

[3]Inspection may test any aspect of the nation's transportation systems, including other aspects of aviation security, such as access controls at airports. However, this statement focuses on Inspection's efforts as they pertain to checkpoint and checked baggage screening procedures.

screening.[4] TSA is currently in the process of transferring covert test programs managed by Security Operations to Inspection for the purposes of improving covert testing and increasing the validity of data collection and reporting.[5] However, until this transfer is complete, both Inspection and Security Operations continue to perform covert tests at the nation's commercial airports using distinct processes.

My statement today summarizes selected findings from our April 2019 report on TSA's covert testing program.[6] Specifically, it addresses the extent to which 1) TSA's covert tests are risk-informed; 2) TSA's covert test processes produced quality information for fiscal years 2016 through March 2018; and 3) TSA has used the results of covert tests to address identified security vulnerabilities. In addition, this statement contains updates from TSA as of June 2019 about actions it has taken to address the recommendations made in our April 2019 report.

For the April 2019 report, we reviewed agency documentation, interviewed agency officials, and observed covert tests conducted by Security Operations and Inspection at five airports. We also analyzed Security Operations' covert test data for fiscal years 2017 and the first half fiscal year 2018, and reviewed Inspection's reports for fiscal years 2016 and 2017 testing. We also reviewed documentation and spoke with TSA officials responsible for an agency-wide process to address vulnerabilities identified through covert testing. Additional details on the

[4]For the purposes of this statement, and unless otherwise noted, references to TSOs include both TSA-employed screening personnel and personnel employed by a private sector company contracted with TSA to perform screening services at airports participating in TSA's Screening Partnership Program. See 49 U.S.C. § 44920. TSA's screening procedures—called standard operating procedures—govern how all screening personnel are supposed to screen passengers, their accessible property, and checked baggage for prohibited and other dangerous items. TSA conducts covert testing at all airports at which TSA screening procedures are implemented.

[5]Given that TSA was in the process of this reorganization at the time of our April 2019 report, our report did not address the full extent of changes resulting from this reorganization. According to TSA officials, upon completion of the reorganization, Inspection will be responsible for all TSA covert testing of checkpoint and checked baggage screening moving forward.

[6]GAO, *Aviation Security: TSA Improved Covert Testing but Needs to Conduct More Risk-Informed Tests and Address Vulnerabilities*, GAO-19-374 (Washington, D.C.: April 4, 2019). This is the public version of a classified report we issued in January 2019. We made nine recommendations to strengthen TSA's covert tests in this report. TSA concurred with all of the recommendations. This hearing statement focuses on the recommendations for which TSA has taken actions or has near-term plans.

scope and methodology are available in our published report. For our updates, we reviewed documentation TSA officials submitted to identify actions taken to address GAO's recommendation.

The work on which this statement is based was conducted in accordance with generally accepted government auditing standards.

TSA Revised Its Covert Test Processes in 2016 and Has Taken Steps to Document and Use a Risk-Informed Approach

Inspection Redesigned Its Covert Test Process to Be More Risk-Informed and Quantitative and Has Taken Steps to Document Its Rationales for Selecting Test Scenarios

In April 2019, we reported that Inspection redesigned its testing process in 2016 to conduct covert tests more consistently across airports, and began using quantitative methods to design tests and analyze results so that its findings might be applied more broadly across airports nationwide. As part of its new testing effort, Inspection recruited a technical team of employees with expertise in statistics and engineering to enhance the design, execution, analysis, and reporting of its covert tests.

We also found that Inspection's new test process considered all three elements of a comprehensive risk assessment—threat, vulnerability, and consequence—when selecting locations (e.g., larger airports vs. smaller airports) and scenarios (i.e., the threat items and screening activities to use for tests) to test. However, we found it had not fully documented this approach. Documenting how it considers each of the three elements of risk when determining what to test would help Inspection program managers ensure that where and what they test is appropriately accounting for risk, as called for by DHS and TSA guidance.

We recommended that TSA document its rationale for key decisions related to its risk-informed approach for selecting covert test scenarios. DHS agreed and has since provided us with program documentation to address the recommendation. We are currently assessing this

information. As such it is not yet clear if TSA's efforts sufficiently address this recommendation.

Security Operations Redesigned Its Covert Tests to Address Prior Deficiencies and Has More Fully Incorporated Known Risks into Its New Process

In our April 2019 report, we found that Security Operations had taken actions to strengthen its covert test program, including issuing new guidance and establishing a parallel test process carried out by headquarters staff to validate (i.e., determine the quality of) the results of covert tests conducted by TSA staff at airports.

Although Security Operations took steps to improve the quality of its test process, we found it had not fully considered risk information when determining what kinds of tests to run. Security Operations officials stated they relied largely on program managers' professional judgment to make decisions about what to test, as opposed to making decisions based on risk assessments. However, we found that Security Operations' selection of threat items (e.g., guns, knives, explosive devices, etc.) for covert tests at the checkpoint in fiscal year 2017 did not fully reflect the threats identified in TSA's 2016 *Transportation Sector Security Risk Assessment*—TSA's primary risk assessment of threats for all transportation modes.[7] Using a risk-informed approach to select scenarios that more fully account for known risks—such as those identified in the *Transportation Sector Security Risk Assessment* or a similar risk assessment—could better ensure that TSA is using its finite testing resources to target screening activities that will counter the most likely threats.

We recommended that TSA incorporate a more risk-informed approach into its process for selecting Security Operations' covert test scenarios. In April 2019, TSA began basing its selection of scenarios for Security Operations' covert tests upon information within TSA's Risk and Trade Space Portfolio Analysis tool, an intelligence and data-driven methodology that utilizes information from multiple TSA risk assessments to prioritize domestic aviation security system vulnerabilities. Under the new process, the number of tests involving a particular threat item and screening process will be informed by the methodology's assessment of the likelihood of such a scenario taking place. TSA's actions have met the intent of our recommendation.

[7]We reviewed the *2016 Transportation Sector Security Risk Assessment*, which would have been available to Security Operations for planning the tests it would conduct for fiscal year 2017.

Inspection's Updated Process Is Designed to Produce Quality Information, but Security Operations Faces Challenges with the Quality of Its Test Results

In our April 2019 report, we found that Inspection had established a new process and principles for conducting covert tests, as well as collecting and analyzing test data. These new processes were intended to result in quality information on screening vulnerabilities. For example, to limit the potential for airport staff to be forewarned of testing, we observed that Inspection conducted tests simultaneously across checkpoints, and concluded testing at the airport after an initial round of testing. In addition, we found that once Inspection completes all tests for a given scenario, it develops classified reports containing the results of its quantitative analysis (including detection rates for specific threat items). As part of its new process, Inspection issued guidance to ensure consistency in analysis and reporting of test results. We reviewed two reports on the results of Inspection's covert testing for fiscal years 2016 and 2017 that were completed using its new processes, and found they resulted in quality information on screening vulnerabilities.[8]

In contrast, we found that Security Operations has not been able to ensure the quality of the results of covert tests performed by TSA staff at local airports. Security Operations established a parallel test process carried out by headquarters staff to validate test results conducted by local TSA staff at airports. According to our analysis of Security Operations national covert test data for fiscal year 2017 and the first half of fiscal year 2018, this process showed that covert tests conducted by local airport staff for checkpoint screening operations did not meet TSA's threshold for quality test information.

We also identified local airport testing practices that could be compromising the quality of test results. For example, we observed tests in which TSOs correctly identified the threat items, but a TSA airport official in charge of testing was present at the checkpoint during the tests, and his presence may have provided advance notice to the TSOs that testing was in progress. Additionally, we learned from airport testing officials that having the test coordinator present at the checkpoint was a routine practice when testing was in progress. At another airport visit, one TSO told us that TSOs often know a test is in progress because TSA airport officials use the same test bag to conceal threat items across all tests performed at the airport. According to TSA documentation, potential

[8]These two reports were based on Inspection testing conducted in fiscal years 2016 and 2017 and were finalized in July 2018. Further information on the reports, such as the titles, was deemed sensitive security information.

lapses in the covertness of covert tests, similar to those we observed and were told about, can make TSOs aware that they are being tested and lead to test results that overstate actual TSO performance. Further, we found that the potential for variability in how TSA staff at local airports build threat items and test bags for tests may affect the quality of the test results.

We recommended that TSA assess the current covert testing process used by TSA officials at airports—including factors that may affect the covertness and consistency of the tests—to identify opportunities to improve the quality of test data. Assessing these processes would help TSA make changes that could improve the quality of tests and associated results. This, in turn, would better position those who use these results (including agency leadership and TSA airport officials) to reliably identify and address any vulnerabilities. DHS agreed with our recommendation and estimated that this effort would be complete by July 31, 2019.

TSA Established A New Process to Address Vulnerabilities, but It Has Made Limited Progress

We also found in our April 2019 report that TSA established the Security Vulnerability Management Process in 2015 to review and address any systemic vulnerability facing TSA, including those identified through Inspection's covert tests. However, this process had not yet resolved any identified security vulnerabilities.[9] TSA created the Security Vulnerability Management Process because the prior process did not provide agency-wide visibility and the level of accountability needed to resolve the vulnerabilities. According to TSA, the new process would better ensure the cooperation of various program offices within TSA that had the expertise needed to address vulnerabilities.

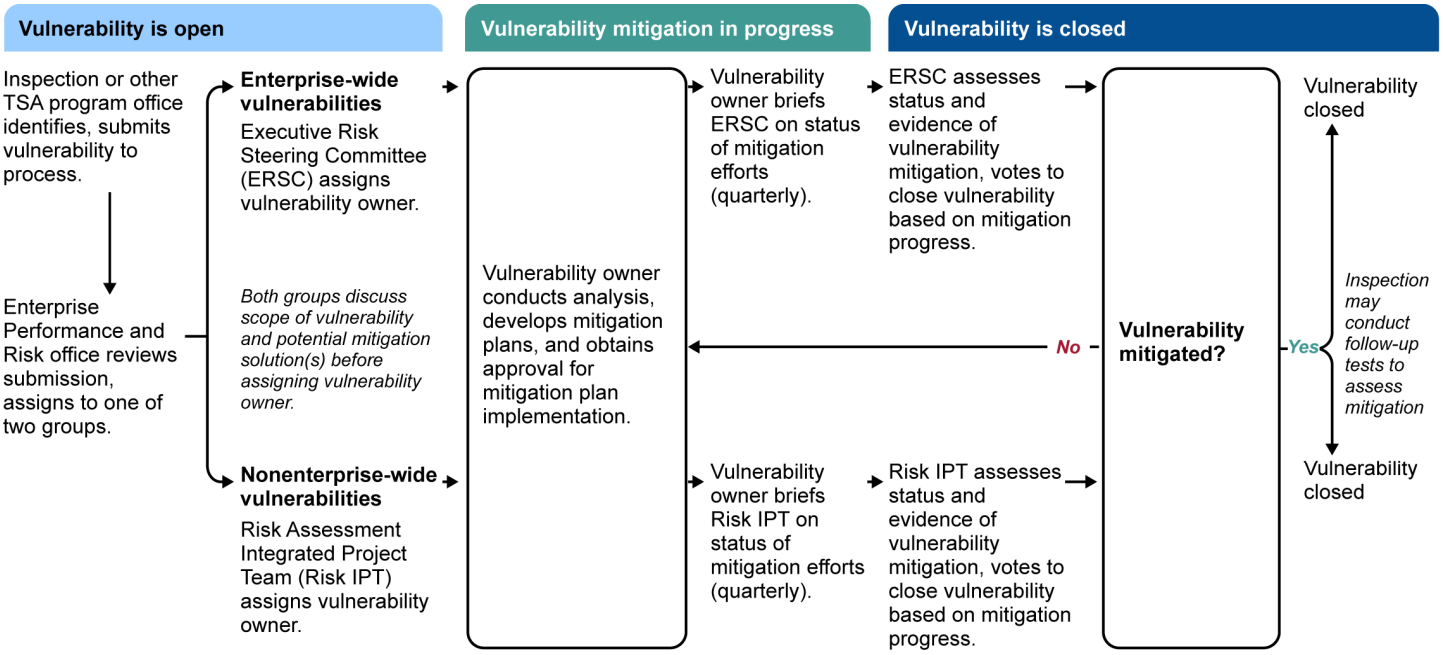
TSA's Strategy, Policy Coordination, and Innovation office is responsible for managing and overseeing the Security Vulnerability Management Process, as well as enforcing deadlines for vulnerability mitigation.[10] When vulnerabilities are submitted to the process, the office submits them for review by one of two groups of TSA stakeholders—the Executive Risk

[9]The process is intended to apply to all evaluations, assessments, and testing of security vulnerabilities conducted by TSA, and is not limited to covert test results or aviation screening activities. Vulnerabilities can be identified, for example, through such things as routine inspections; investigations of employee misconduct and employee fraud; internal audits; and program office assessments.

[10]The TSA Strategy, Policy Coordination, and Innovation office is under the purview of the TSA Administrator's Chief of Staff.

Steering Committee or the Risk Assessment Integrated Project Team.[11] These two groups are responsible for identifying all TSA program offices affected by the vulnerability in question and assigning a vulnerability owner, which has responsibility for developing and leading mitigation efforts for a specific vulnerability. The vulnerability owner then works with program offices to determine whether and how vulnerabilities can be mitigated and formally closed through the process (see fig. 1).

Figure 1: The Transportation Security Administration (TSA) Security Vulnerability Management Process



Source: GAO analysis of TSA documentation. | GAO-19-633T

We reviewed the vulnerabilities that Inspection has submitted to the process, and, as of June 2019, none of the vulnerabilities had been

[11]The Executive Risk Steering Committee, which is composed of Assistant Administrators who lead TSA's program offices, reviews vulnerabilities known as enterprise risks, which are risks involving terrorism threats to the entire transportation sector or that negatively impact TSA's ability to achieve its mission. TSA's Risk Assessment Integrated Project Team, composed of members from each TSA program office, reviews all vulnerabilities determined not to be enterprise wide.

closed through mitigation steps taken through the process.[12] Specifically, 8 vulnerabilities Inspection has submitted to the process have been in progress from 13 to 39 months. We also reported that 3 vulnerabilities had been waiting for vulnerability owners to be assigned for a period of 4, 5, and 7 months, respectively before TSA assigned them vulnerability owners in September 2018.

We found that TSA has had difficulty closing identified vulnerabilities through the Security Vulnerability Management Process, in part, because it did not establish timeframes and milestones to ensure offices responsible for vulnerabilities are making measured progress toward mitigation. Moreover, we found that the process charter did not establish a method for how the office or entity managing the process is to monitor mitigation activities to ensure that responsible TSA program offices are meeting any identified timeframes and milestones. In our April 2019 report, we noted that such methods could include identifying a person or entity responsible for escalating cases when these timeframes are not being met.

TSA officials told us that timeframes for vulnerability mitigation can vary due to the number of stakeholders and the complexity of certain threats, especially those involving technology solutions. Additionally, they cited factors beyond TSA's control that can delay mitigation efforts, such as changes to agency leadership and personnel changes. Inspection officials told us that while officials are working on mitigation solutions for identified vulnerabilities, Inspection will assist TSA program offices with implementing interim mitigation procedures before formal mitigation plans are developed. However, in some cases Inspection's findings represent system-wide vulnerabilities to commercial aviation that could result in potentially serious consequences for TSA and the traveling public. For this reason, it is important that TSA make timely progress on formal mitigation solutions.

We recommended that DHS establish time frames and milestones for key steps in the Security Vulnerability Management Process and that it revise existing guidance for the process to establish procedures for monitoring vulnerability owner's progress against timeframes and milestones. DHS concurred with our recommendation. In June 2019, TSA provided us with

[12]Inspection submitted nine vulnerabilities in total. We found that TSA closed one of the nine vulnerabilities 2 years after submission to this process because the relevant program office made policy changes that addressed Inspection's interim findings.

a revised charter for the Security Vulnerability Management Process that established timeframes and milestones for key aspects of the process, such as assigning a vulnerability owner. TSA's actions have met the intent of our recommendation.

Chairman Cummings, Ranking Member Jordan, and Members of the Committee this completes my prepared statement. I would be pleased to respond to any questions that you may have at this time.

GAO contact and Staff Acknowledgments

If you or your staff members have any questions about this testimony, please contact me at (202) 512-7331 or johnsoncm@gao.gov. Contact points for our Offices of Congressional and Public Affairs may be found on the last page of this statement. Other individuals making key contributions to this work include William Russell, Acting Director; Ellen Wolfe, Assistant Director; Mona Nichols Blake, Analyst-in-Charge; Jason Blake; Michele Fejfar; Erin O'Brien; Susan Hsu; Tom Lombardi; and Chuck Bausell.