United States Government Accountability Office

GAO

Testimony

Before the Committee on Oversight and Government Reform, House of Representatives

For Release on Delivery
Expected at 10:00 a.m. EST
Thursday, November 15, 2007

AVIATION SECURITY

Vulnerabilities Exposed Through Covert Testing of TSA's Passenger Screening Process

Statement of Gregory D. Kutz, Managing Director
Forensic Audits and Special Investigations

John W. Cooney, Assistant Director
Forensic Audits and Special Investigations

GAO

Accountability * Integrity * Reliability

GAO-08-48T

November 15, 2007

AVIATION SECURITY

Vulnerabilities Exposed through Covert Testing of TSA's Passenger Screening Process

GAO Accountability · Integrity · Reliability

Highlights

Highlights of GAO-08-48T, a testimony before the Committee on Oversight and Government Reform, House of Representatives

Why GAO Did This Study

In August 2006, the Transportation Security Administration (TSA) substantially modified its passenger screening policies based on the alleged transatlantic bomb plot uncovered by British authorities. With the aim of closing security gaps revealed by the alleged plot, the revised policies severely restricted the amount of liquids, gels, and aerosols TSA allowed passengers to bring through the checkpoint.

At the Committee's request, GAO tested whether security gaps exist in the passenger screening process. To perform this work, GAO attempted to (1) obtain the instructions and components needed to create devices that a terrorist might use to cause severe damage to an airplane and threaten the safety of passengers and (2) test whether GAO investigators could pass through airport security checkpoints undetected with all the components needed to create the devices.

GAO conducted covert testing at a nonrepresentative selection of 19 airports across the country. After concluding its tests, GAO provided TSA with two timely briefings to help it take corrective action. In these briefings, GAO suggested that TSA consider several actions to improve its passenger screening program, including aspects of human capital, processes, and technology. GAO is currently performing a more systematic review of these issues and expects to issue a comprehensive public report with recommendations for TSA in early 2008.

To view the full product, including the scope and methodology, click on GAO-08-48T. For more information, contact Gregory D. Kutz at (202) 512-6722 or kutzg@gao.gov.

What GAO Found

GAO investigators succeeded in passing through TSA security screening checkpoints undetected with components for several improvised explosive devices (IED) and an improvised incendiary device (IID) concealed in their carry-on luggage and on their persons. The components for these devices and the items used to conceal the components were commercially available. Specific details regarding the device components and the methods of concealment GAO used during its covert testing are classified by TSA; as such, they are not discussed in this testimony.

Using publicly available information, GAO investigators identified two types of devices that a terrorist could use to cause severe damage to an airplane and threaten the safety of passengers. The first device was an IED made up of two parts—a liquid explosive and a low-yield detonator. Although the detonator itself could function as an IED, investigators determined that it could also be used to set off a liquid explosive and cause even more damage. In addition, the second device was an IID created by combining commonly available products (one of which is a liquid) that TSA prohibits in carry-on luggage. Investigators obtained the components for these devices at local stores and over the Internet for less than $150. Tests that GAO performed at a national laboratory in July 2007, in addition to prior tests in February 2006 that GAO performed in partnership with a law enforcement organization in the Washington, D.C., metro area, clearly demonstrated that a terrorist using these devices could cause severe damage to an airplane and threaten the safety of passengers.

Investigators then devised methods to conceal the components for these devices from TSA transportation security officers, keeping in mind TSA policies related to liquids and other items, including prohibited items. By using concealment methods for the components, two GAO investigators demonstrated that it is possible to bring the components for several IEDs and one IID through TSA checkpoints and onto airline flights without being challenged by transportation security officers. In most cases, transportation security officers appeared to follow TSA procedures and used technology appropriately; however, GAO uncovered weaknesses in TSA screening procedures and other vulnerabilities as a result of these tests. For example, although transportation security officers generally enforced TSA's policies, investigators were able to bring a liquid component of the IID undetected through checkpoints by taking advantage of weaknesses identified in these policies. These weaknesses were identified based on a review of public information. TSA determined that specific details regarding these weaknesses are sensitive security information and are therefore not discussed in this testimony. GAO did not notice any difference between the performance of private screeners and transportation security officers during our tests.

Mr. Chairman and Members of the Committee:

Thank you for the opportunity to discuss our latest test of airport security. In March 2006, we reported on the results of covert security vulnerability testing at 21 airports across the country. These tests clearly demonstrated that our nation's airlines were vulnerable to a suicide bomber using commercially available materials to detonate an explosive device onboard an airplane. During these covert tests, our investigators passed through airport security checkpoints carrying prohibited explosive components without being caught by Transportation Security Administration (TSA) security officers.[1] Later that year, in August 2006, British authorities uncovered the alleged transatlantic bomb plot. The discovery of this bomb plot, in which terrorists allegedly sought to detonate improvised explosive devices (IED)[2] in airplanes as they crossed the Atlantic Ocean, caused TSA to substantially modify its screening procedures—all liquids, gels, and aerosols with some exceptions were banned from being carried through passenger screening checkpoints and onto aircraft until the plot was further investigated. These restrictions were later relaxed to allow small amounts of liquids, gels, and aerosols through the checkpoint.

This report responds to your request that we test whether security vulnerabilities exist in the TSA passenger screening process. To perform this work, we attempted to (1) obtain the instructions and components needed to create devices that a terrorist might use to cause severe damage to an airplane and threaten the safety of passengers and (2) test whether investigators could pass through airport security checkpoints undetected with all the components needed to create the devices.

To obtain instructions on creating devices a terrorist might use, we reviewed publicly available information and performed Internet searches. We obtained components for these devices at local stores and over the Internet. We devised methods to conceal the prohibited components using public information about TSA policies and procedures and obtained items to conceal the components at local stores and over the Internet. We then conducted our covert tests at a nonrepresentative selection of 19 airports

[1]Our March 2006 report is classified, but TSA has authorized this limited discussion.

[2]An IED is an apparatus or contraption placed or fabricated without detailed manufacturing that incorporates destructive, lethal, noxious, pyrotechnic, or incendiary chemicals and is designed to destroy, incapacitate, or distract through high-speed projectiles and overpressure.

across the country. The criteria we used to select the airports resulted in our testing a variety of U.S. commercial airports, some of which employed private screeners.[3]

Our work was not intended to evaluate the overall design and effectiveness of TSA's airport security program, which contains multiple layers of security. Rather, our work was performed to test specific security vulnerabilities related to the three major elements of TSA's passenger screening process—human capital (i.e., people), processes, and technology employed at the checkpoint. We tested the effectiveness of our explosive device at a national laboratory in July 2007. We had previously tested the effectiveness of less powerful explosive and incendiary devices in the Washington, D.C., metro area with help of a local law enforcement organization. We conducted work for this investigation from March 2007 through July 2007 in accordance with quality standards for investigations as set forth by the President's Council on Integrity and Efficiency.

Summary

Our investigators succeeded in passing through TSA security screening checkpoints undetected with components for several IEDs and an improvised incendiary device (IID)[4] concealed in their carry-on luggage and on their persons. The components for these devices and the items used to conceal the components were commercially available. Specific details regarding the device components and the methods of concealment we used during our covert testing are classified by TSA; as such, they are not discussed in this testimony.

Using publicly available information, our investigators identified two types of devices that a terrorist could use to cause severe damage to an airplane and threaten the safety of passengers. The first device was an IED made up of two parts—a liquid explosive and a low-yield detonator. Although the detonator itself could function as an IED, investigators determined that it could also be used to set off a liquid explosive and cause even more

[3]Specific details about which airports employed private screeners as opposed to transportation security officers are considered sensitive security information and are not included in this testimony. Therefore, the term transportation security officer is used throughout this testimony, but may, in some cases, also refer to private screeners that we tested.

[4]A IID is an apparatus or contraption placed or fabricated without detailed manufacturing that incorporates destructive, lethal, noxious, pyrotechnic, or incendiary chemicals and is designed to destroy, incapacitate, or distract by creating intense heat or fire.

damage. In addition, the second device was an IID created by combining commonly available products (one of which is a liquid) that TSA prohibits in carry-on luggage. Investigators obtained the components for these devices at local stores and over the Internet for less than $150. Tests that we performed at a national laboratory in July 2007, in addition to prior tests in February 2006 that we performed in partnership with a law enforcement organization in the Washington, D.C., metro area, clearly demonstrated that a terrorist using these devices could cause severe damage to an airplane and threaten the safety of passengers.

Investigators then devised methods to conceal the components for these devices from TSA transportation security officers, keeping in mind TSA policies related to liquids and other items, including prohibited items. By using concealment methods for the components, two investigators demonstrated that it is possible to bring the components for several IEDs and one IID through TSA checkpoints and onto airline flights without being challenged by transportation security officers. In most cases, transportation security officers appeared to follow TSA procedures and used technology appropriately; however, we uncovered weaknesses in TSA screening procedures and other vulnerabilities as a result of these tests. For example, although transportation security officers generally enforced TSA's policies, investigators were able to bring a liquid component of the IID undetected through checkpoints by taking advantage of weaknesses identified in these policies. These weaknesses were identified based on a review of public information. TSA determined that specific details regarding these weaknesses are sensitive security information and are therefore not discussed in this testimony. We did not notice any difference between the performance of private screeners and transportation security officers during our tests.

We provided TSA officials with two timely briefings to help them take corrective action. While we understand that TSA faces a significant challenge in balancing security concerns with efficient passenger movement, we are recommending that the Secretary of Homeland Security consider several actions to improve aspects of TSA's passenger screening program, including elements of human capital, processes, and technology.

Background

TSA is responsible for securing all modes of transportation while facilitating commerce and freedom of movement for the traveling public. In performing its responsibilities, TSA is guided by risk-based planning, which generally involves a consideration of threats, vulnerabilities, and the criticality or consequence of an attack if it were to be carried out.

transportation security officers attempt to detect prohibited items that passengers may try to carry beyond the security checkpoint.

- **Technology** is used during the screening process, which primarily consists of walk-through metal detectors, X-ray machines, handheld metal detectors, and explosive trace detection (ETD) equipment.[7]

- **Standard operating procedures** establish the process and standards by which transportation security officers are to screen passengers and their carry-on items at screening checkpoints.

The process of screening a passenger who continues to alarm the walk-through metal detector provides an example of how these three elements intersect. According to TSA's Screening Checkpoint Standard Operating Procedures manual, a passenger who continues to alarm the walk-through metal detector must be screened using a hand-wand search. Passengers may alternatively request a full-body pat-down search. The manual describes the process that transportation security officers are to follow during the additional screening, which includes the use of ETD swabbing and a pat-down of the passenger to detect any irregularities in their body contour that could represent concealed items.

TSA Efforts to Improve the Passenger Screening Process

TSA faces a significant challenge in balancing security concerns with efficient passenger movement. In our April 2007 report, we described how TSA monitors transportation security officer compliance with passenger checkpoint screening procedures through its performance accountability and standards system and through testing.[8] Compliance assessments include quarterly observations of transportation security officers' ability to perform particular screening functions in the operating environment, quarterly quizzes to assess their knowledge of procedures, and an annual knowledge and skills assessment. TSA conducts tests to evaluate, in part, the extent to which transportation security officers are able to detect simulated threat items hidden in accessible property or concealed on a person. TSA modifies its standard operating procedures based on the

[7]ETD works by detecting explosive vapors and residue. Human operators collect samples by rubbing swabs along an object, such as a carry-on suitcase. They then place the swabs in an ETD machine. The ETD machine chemically analyzes the swab to identify traces of explosive materials.

[8]GAO-07-634.

Specifically, in its approach to securing the domestic aviation sector, TSA maintains numerous programs that provide a layered approach to security, including intelligence gathering and analysis, checking passenger manifests against watch lists, and assigning undercover air marshals to certain flights. The general public associates TSA mainly with its security effort at airport passenger checkpoints. One primary goal of the passenger checkpoint screening program is to provide for the safety and security of persons and property on an aircraft against the introduction of an unauthorized weapon, explosive, or incendiary.[5] As we reported in April 2007, TSA continues to modify its checkpoint screening program based on a number of factors including passenger feedback, risk-based planning, and its own internal review and testing process.[6] TSA's well-publicized recent policy change in response to the alleged transatlantic bomb plot of August 2006 is an important example of risk-based planning. Known as the 3-1-1 rule, this procedural change prohibits liquid, gel, or aerosol items over 3.4 fluid ounces in carry-on luggage; in addition, all liquid and gels should be placed in a 1-quart bag, and only one 1-quart bag is allowed per passenger.

Passenger Screening Process

TSA focuses on the checkpoint screening process as a primary means of detecting prohibited items. Items that TSA has prohibited passengers from bringing aboard an aircraft include, among other things, firearms and knives; gasoline and lighter fluid; disabling chemicals, including chlorine and liquid bleach; and many additional items that may be seemingly harmless but could be used as weapons. During the passenger screening process, transportation security officers follow standard operating procedures and utilize technology such as walk-through metal detectors and X-ray machines to detect prohibited items either on a passenger's person or in his or her carry-on luggage. The passenger checkpoint screening process is composed of the following three elements:

- **Transportation security officers** (also known as TSOs) screen all passengers and their carry-on luggage prior to allowing passengers access to their departure gates. Among other responsibilities,

[5]49 C.F.R. §§ 1542.101, 1540.107, and 1540.111.

[6]GAO, *Aviation Security: Risk, Experience, and Customer Concerns Drive Changes to Airline Passenger Screening Procedures, but Evaluation and Documentation of Proposed Changes Could Be Improved*, GAO-07-634 (Washington, D.C.: Apr. 16, 2007).

professional judgment of TSA senior-level officials and program-level staff, daily experiences of airport staff, complaints and concerns raised by the traveling public, and an analysis of risks to the aviation system. For example, in December 2005, TSA modified its prohibited items list to allow passengers to carry certain scissors and tools as long as they did not exceed a certain length. TSA's stated purpose in removing certain scissors and tools from the prohibited items list was to shift the focus of transportation security officers from items considered by TSA to pose a low threat to items considered to pose a high threat.

Creating Functioning IED and IID Devices

Investigators found instructions on the Internet for creating both an IED and IID and purchased the components from the Internet and from a local store for approximately $150. The IED was conceived as a two-part device—a detonator component that, on its own, could function as an IED, and a mixture of fuel and oxidizer that would require the explosion of the detonator.[9] Although the detonator component could be considered an IED, for the purposes of this report, we are referring to the combination of the detonator and the liquid explosive as a single IED. Information about liquid explosives was publicly available on several Web sites and discussed in media articles related to various terror plots, including the failed London subway bombing of July 21, 2005, and the transatlantic bomb plot of August 2006. In addition, we obtained information about creating an IID from the Internet. We also found videos on the Internet of the intense fire resulting from an IID. One of the components for the IID is a liquid that TSA prohibits passengers from bringing through security checkpoints. Specific details regarding the device components and the methods of concealment we used during our covert testing are classified by TSA; as such, they are not discussed in this testimony.

A group of tests conducted in February 2006 and July 2007 show that the IED proposed for this investigation functions as intended. In 2006, within the scope of our original covert testing report, we worked with a law enforcement organization in the Washington, D.C., metro area to confirm that the detonator would function as an IED. A test performed by local law enforcement officials confirmed that the detonator would cause damage to an aircraft and threaten the safety of passengers. Because our proposed IED for this investigation was composed of two parts (the detonator and

[9]Many chemical explosives consist of a mixture of oxidizer and fuel. When heat is added to the mixture, an explosion occurs.

the liquid explosive), in July 2007 we sought assistance to confirm that this more complex IED would function as intended. Several tests conducted at a national laboratory demonstrated that this IED can function as intended, with the initial explosion by the detonator successfully causing the liquid explosive to detonate in several tests. Explosion data indicate that this device exploded with a force sufficient to cause severe damage to an aircraft. The IID is a far simpler device. Our work with a law enforcement organization in the Washington, D.C., metro area in February 2006 confirmed that the components of the IID (one of which is a liquid) could function as intended, causing damage to an aircraft and threatening the safety of passengers.

Testing at 19 Airport Security Checkpoints

Our investigators devised methods that would allow them to conceal the prohibited components for these devices from transportation security officers. During this planning phase, they considered publicly advertised TSA policies related to liquids and other items, including prohibited items. They also judged that some components could be hidden in either their carry-on luggage or on their persons. They developed covert test procedures to challenge TSA screening measures using these components and methods. Specific details regarding the methods of concealment we used are classified by TSA; as such, these details are not discussed in this testimony.

By using various concealment methods, our investigators demonstrated that it is possible to bring the components for several functioning IEDs and one functioning IID through checkpoints and onto airline flights without being challenged by transportation security officers. In most cases, transportation security officers appeared to follow TSA procedures and used technology appropriately; however, we uncovered weaknesses in TSA screening procedures and other vulnerabilities as a result of these tests. For example, although transportation security officers generally enforced TSA's 3-1-1 rule, we were able to bring a liquid component of the IID undetected through checkpoints by taking advantage of weaknesses we identified in TSA's policies based on a review of public information. TSA determined that specific details regarding these weaknesses are sensitive security information and are therefore not discussed in this testimony. We did not notice any difference between the performance of private screeners and transportation security officers during our tests.

Covert Test Series One

From March 19 through March 23, 2007, two investigators tested the TSA checkpoint screening process at a number of U.S. airports. Transportation

security officers did not interact with our investigators at every airport. Interactions that did occur included the following:

- On March 19 and March 20, 2007, transportation security officers advised our investigators to use a 1-quart clear plastic bag rather than the larger bags they were using, but did not require them to do so before passing through the checkpoint.

- Also at another airport, on March 23, 2007, a transportation security officer did not allow one investigator to bring a small, unlabeled bottle of medicated shampoo through the checkpoint. This was a legitimate toiletry item used by one of our investigators. The officer cited TSA policy and stated that since the bottle was not labeled, "it could contain acid." She did not allow our investigator to bring the unlabeled medicated shampoo bottle through the checkpoint. However, a liquid component of the IID—despite being prohibited by TSA—was allowed to pass undetected through the checkpoint. We had identified this weakness based on a review of public information before performing our tests.

Covert Test Series Two

From May 7 through May 9, 2007, two investigators tested the TSA checkpoint screening process at a number of U.S. airports. Transportation security officers did not interact with our investigators aside from the following:

- On May 8, 2007, one investigator deliberately placed coins in his pockets to ensure that he would receive a secondary inspection. The transportation security officer used a hand-wand and performed a pat-down search of our investigator. However, the transportation security officer did not detect any of the prohibited items our investigator brought through the checkpoint.

Covert Test Series Three

From June 5 through June 8, 2007, two investigators tested the TSA checkpoint screening process at a number of U.S. airports. Transportation security officers did not interact with our investigators at every airport. Interactions that did occur included the following:

- Inclement weather forced our investigators to change their flight plans at one airport. After changing their plans, they were selected for secondary inspection at the TSA security checkpoint. Transportation security officers performed pat-downs at the checkpoint. However, the

transportation security officers did not detect any of the prohibited items our investigators brought through the checkpoint.

Corrective Action Briefings

We briefed TSA officials on August 16, 2007, and September 5, 2007, to discuss our findings. Officials from TSA's Security Operations Office were present during our second briefing. At these briefings, we suggested that TSA consider how the results of our covert testing should affect its risk-based approach to airport security. This could include implementing one or more measures to reduce the likelihood that terrorists could successfully bring IED and IID components through checkpoints using a similar methodology to ours in the future.

The specific nature of our suggestions to TSA is considered sensitive security information. Put generally, we suggested that, among other things, TSA (1) establish, depending on airport capacity, one or more special passenger screening lines to screen individuals based on risk and individuals with special needs; (2) introduce more aggressive, visible, and unpredictable deterrent measures into the passenger screening process at airports nationwide, to potentially include the implementation of enhanced individual search procedures (e.g., pat-downs and hand-wand screening) to detect concealed components; and (3) continue to develop and deploy new technology to be used at passenger screening checkpoints that would be able to better detect concealed components.

TSA officials indicated that they did not disagree with our suggestions in principle and that they would examine them closely to determine whether and how they should be implemented. They acknowledged vulnerabilities in human capital, processes, and technology. They also indicated that they are deploying additional specialized personnel to enhance security at existing checkpoints and that they are exploring methods for enhancing transportation security officer training and transforming the culture of their workforce. Regarding standard operating procedures, officials said that they are continuously revisiting and revising their policies. They also indicated that they were moving forward to develop a "checkpoint of the future" that would incorporate new and emerging technology to address terror threats. Such technology could include innovative imaging techniques.

Conclusion

Our tests clearly demonstrate that a terrorist group, using publicly available information and few resources, could cause severe damage to an airplane and threaten the safety of passengers by bringing prohibited IED