U.S. House of Representatives
Committee on Transportation and Infrastructure
Washington, DC 20515

James L. Oberstar
Chairman

David Heymsfeld, Chief of Staff
Ward W. McCarragher, Chief Counsel

John L. Mica
Ranking Republican Member

James W. Coon II, Republican Chief of Staff

July 23, 2008

SUMMARY OF SUBJECT MATTER

TO: Members of the Subcommittee on Aviation

FROM: Subcommittee on Aviation Staff

SUBJECT: Hearing on "Aviation Security: An Update"

PURPOSE OF HEARING

The Subcommittee will meet on Thursday, July 24, 2008, at 10:00 a.m. in room 2167 Rayburn House Office Building to receive testimony regarding Aviation Security: An Update.

BACKGROUND

Before the terrorist attacks of September 11, 2001, aviation security in the United States was shaped largely as a result of past events such as the proliferation of domestic hijackings between 1961 and 1972 and the 1988 bombing of Pan Am flight 103[1]. In response to these incidents, metal detectors and X-rays were installed to find guns and other weapons, and investments in research and development were made to find new technology and equipment to indentify additional items that posed an aviation security threat. Following the attacks of September 11, 2001, the *Aviation and Transportation Security Act* (*ATSA*, P.L. 107-71) made significant changes to aviation security policy and strategy, including federalizing the screener workforce and requiring 100 percent screening of carry-on and checked baggage. The 9/11 Commission Report issued on July 22, 2004, stated that the Transportation Security Administration (TSA) had not yet created a comprehensive plan for aviation.[2] In response, Congress passed the *Intelligence Reform and Terrorism Prevention Act of 2004* (*IRTPA* P.L. 108-458) to require the Secretary of Homeland Security and the Secretary of Transportation to work jointly on such a strategy. The Department of Homeland Security (DHS)

[1] Pan Am flight 103 crashed into the city of Lockerbie, Scotland after a bomb in the luggage compartment exploded, the crash killed all 259 passengers and 11 people on the ground.

[2] Final Report of the National Commission on Terrorist Attacks Upon the United States, *The 9/11 Commission Report*, 390-391, (W.W. Norton & Company, July 22, 2004).

was directed by the Bush Administration to create a national strategy and comprehensive plan for aviation security in June of 2006. The strategy became National Security Presidential Directive 47/Homeland Security Presidential Directive 16 (NSPD-47/HSPD-16).[3] On March 26, 2007, the National Strategy for Aviation Security was released, the strategy aligns Federal government aviation security programs and initiatives into a comprehensive and cohesive national effort involving appropriate federal, state, local, and tribal governments and the private sector to provide active layered aviation security for the United States.[4]

I. Screening Procedures and Technologies

A. Passenger and Carry-on Baggage Screening

Current checkpoint passenger screening consists of going through a metal detector, which are used to identify metals on passengers. If metal is found, a secondary screening is performed by wanding the passenger and a physical pat-down is performed. This is fundamentally pre-9/11 technology. By the end of 2008, TSA states that over half of the travelers will be screened by advanced technology X-ray, the majority will be observed by behavior detection officers, and 100 percent will be checked by document checkers.

To strengthen checkpoint passenger screening, two new technologies are currently being piloted in the screening process, including X-ray backscatter and Millimeter Wave Imaging Systems. X-ray backscatter technology measures the scatter or reflections of the X-ray beam differentiating the organic materials (different chemical elements in these materials scatter the X-ray in different patterns). Millimeter wave screening technology refers to a wide array of screening devices capable of creating highly detailed images by measuring the reflections of ultra high frequency (i.e., in the 30-300 giga-Hertz frequency range) waves emitted by the system that are capable of passing through barriers that normally preclude visual inspection.

At the security checkpoint, passengers' carry-on property is also screened. Passengers remove shoes, coats, and other items, which are sent through an X-ray machine along with bags, purses, computers and other carry-on items.

On April 28, 2008, TSA introduced the Checkpoint Evolution prototype at the Baltimore-Washington International Thurgood Marshall Airport (BWI), with the goal of introducing new technologies such as the Millimeter Wave, multi-view X-ray, and liquid bottle scanners at one checkpoint. BWI managers completed a 16-hour training program to incorporate the latest intelligence analysis, explosive detection, and also received interpersonal communication training to create a calm checkpoint environment to better identify unusually nervous or incongruous behavior.

According to TSA, it will continue to test emerging technologies -- such as whole body imagers, explosives trace portals, cast and prosthesis scanners, next generation explosives trace detection equipment, automated carry-on baggage explosives detection systems, advanced technology X-ray systems, and bottle liquid scanners. According to TSA, it has not yet identified the technology solutions it believes would be appropriate for wide scale purchase and deployment.

[3] President George W. Bush, *National Security Presidential Directive/NSPD-47, Homeland Security Presidential Directive/HSPD-16, Subject: Aviation Security Policy*, Washington, DC: The White House, June 20, 2006.

[4] U.S. Department of Homeland Security, *The National Strategy for Aviation Security*, March 26, 2007, at 1.

B. Checked Baggage Screening

The *ATSA* required screening of all checked baggage by Explosive Detection Systems (EDS). EDS systems use X-ray computed tomography to scan objects, and computational algorithms that assess the probability of threat object detection based on object density characteristics. Certified EDS systems must meet acceptable detection and false alarm rates for bulk explosive detection. While most specific performance criteria of certified EDS systems are classified, EDS systems used for checked baggage must meet or exceed a throughput rate of 450 bags per hour.

In the last few years, there have been numerous findings from the 9/11 Commission, the Government Accountability Office (GAO), and TSA that document the benefits of moving EDS machines from airport lobbies and placing them in-line with baggage conveyor systems and behind ticket counters. These benefits include:

- ***Increased Baggage Throughput***: Baggage throughput would be increased from 150 bags per hour with current lobby installations to 450-600 bags per hour with high speed in-line systems.

- ***Reduced TSA Operating Costs***: GAO reports that TSA has estimated that in-line baggage screening systems at the 9 airports that received federal funding through letter of intent (LOI) agreements could save the Federal Government approximately $1.3 billion over the next 7 years.

- ***Increased Security***: Moving explosives units into a secured area will promote greater security because: 1) screening machines will not be exposed to the public; 2) screeners will be able to focus on screening bags rather than moving them; and 3) fewer people will be congregated around machines in the public area.

Between fiscal year (FY) 2002 and FY 2006, Congress appropriated a total of $2.078 billion for EDS-related terminal modifications, although more than $500 million of those funds (mostly in FY 2002) were dedicated to moving the machines into airports to meet statutory deadlines for electronically screening checked baggage.

TSA and airport operators rely on LOI agreements as the principal method of federal funding for the modification of airport facilities to incorporate in-line baggage screening systems. As of January 2003, TSA issued 8 letters of intent to cover the costs of installing systems at 9 airports for a total cost to the Federal Government of $957.1 million over 4 years. No new LOIs have been issued since.

At the end of FY 2006, 36 airports had operational in-line systems – 18 airports with full systems and 18 airports with partial systems (terminal solutions). Over the next year, TSA expects full and partial in-line systems to become operational at 25 additional airports.

In February 2006, TSA completed its *Strategic Planning Framework for the Electronic Baggage Screening Program*, which provides a deployment strategy for in-line EDS. The plan provides optimal screening solutions – e.g. high speed in-line, micro in-line (i.e., behind the ticket counter), stand alone EDS -- for 250 airports. Additionally, the plan provides a list of the top 25 priority airports. TSA officials estimate that it will cost approximately $4 to $6 billion (purchase, installation and associated infrastructure upgrades) to achieve its optimal solution by 2019.

C. Employee Screening Pilot Program

According to TSA, it currently deploys a layered approach to employee security that includes random and roving screening, checkpoint screening for certain populations, and "surge" inspections.[5] TSA requires employees at an airport with a badge to clear a security threat assessment before a badge can be issued. Audits are underway at airport badge offices across the country to verify adherence to this measure.

The FY 2008 *Consolidated Appropriations Act* (P.L. 110-161) required TSA to create a pilot program to evaluate 100 percent employee screening at three airports and alternative employee screening at four other airports for 90 days, and submit a report to Congress with cost and effectiveness results by September 1, 2008. In May of 2008, 100 percent employee screening began at Boston's Logan International (BOS), Jacksonville (Florida) International, and Craven Regional (New Bern, North Carolina). At the same time, a variation of random screening, behavior detection programs, employee security awareness training, deployment of portable screening equipment, and or the use of biometric access control began at Denver International (DEN), Kansas City (Missouri) International, Eugene (Oregon), and Southwest Oregon Regional (North Bend, Oregon).

D. Transportation Security Officers (TSOs) Staffing

There are over 43,000 TSOs nationwide at approximately 400 airports. TSOs are trained on the latest checkpoint technology, behavioral recognition, and screening techniques. Each TSO must pass a recertification each year. Since 2004, TSA has used a Staffing Allocation Model (SAM) to determine appropriate staffing levels at airports. Although there have been many concerns about staffing levels at particular airports, the GAO found in 2006 that TSA's SAM model was more accurate at predicting staffing needs than previous models. There continue to be some concerns, however, related to the assumed number of part-time TSOs, the timing of the annual allocation, and the process for making staffing adjustments.

E. Crew Personnel Advanced Security System (CrewPASS)

The *9/11 Commission Recommendation Act of 2007 (9/11 Commission Act,* P.L. 110-53*)*, mandates that TSA report to Congress on its "efforts to institute a sterile area access system or method that will enhance security by properly identifying authorized airline flight deck and cabin crew members at screening checkpoints and granting them expedited access through screening checkpoints." Using the existing Cockpit Access Security System (CASS) data and technology, the Air Line Pilots Association collaborated with TSA to create a pilot program to expedite pilots at airport screening checkpoints. On July 17, 2008, CrewPASS was implemented at three locations: BWI, Pittsburgh International Airport, and Columbia (South Carolina) Metropolitan Airport. Eligible flight crew members must present two forms of identification (airline-issued ID and driver's license or passport) to TSOs at the exit lane of the security checkpoint. TSOs check these credentials via a

[5] Press Release, TSA, *TSA to Pilot Airport Employee Screening at Seven Airports,* (Feb. 11, 2008), http://www.tsa.gov/press/releases/2008/0211.shtm.

secure, real-time flight deck crew member database that includes a picture and other information to verify the individual's identity and employment status. Pilots who utilize the program are still subject to random screening, observation by behavior detection officers and other layers of security.

F. Registered Traveler (RT) program

The TSA and private industry developed the RT[6] program to provide an accelerated security screening for passengers who agree to undergo a TSA-conducted security threat assessment (STA) to confirm that they do not pose, nor are suspected of posing, a threat to transportation or national security. TSA is responsible for setting program standards of this market driven private-sector run program, conducting the STA, physical screening at TSA checkpoints, and certain forms of oversight. The private sector is responsible for enrollment, verification, and related services.

Applicants provide RT participating airports/air carriers and service providers (TSA-approved vendors) with biographic and biometric data needed for TSA to conduct the STA and determine eligibility. The STA includes inspection of each applicant's identity against terrorist-related, law enforcement, and immigration databases that TSA maintains or uses.

Once an applicant qualifies for RT, the traveler is able to take advantage of the benefits of the RT program, such as modified airport configuration to minimize RT passenger wait times, including dedicated or integrated lines and lanes. Other potential benefits incorporate enhanced customer service for RT participants, such as additional assistance, concierge service for luggage, parking privileges, and discounts for service or concessions. Additional benefits will depend on the ability of the private sector to identify and invest in innovations that TSA would approve.

The current phase of the RT program, known as the Registered Traveler Interoperability Pilot (RTIP), introduces interoperability among participating airports/air carriers. The RTIP is expected to include roughly 10-20 sponsoring entities. Several sponsoring entities are already operating the RT program at their respective locations. On July 23, 2008, TSA announce that it is ending the pilot and clearing the way for expansion of the RT program while limiting its involvement in the program.

G. Biometrics

Biometrics requirements for use in airport access control and credentialing was included in both *ATSA* and *IRTPA*. *IRTPA* required TSA to provide for the use of biometrics for both airport access control and law enforcement officer travel. While TSA has issued biometric standards, it had not issued performance standards to allow airports to make decisions about which biometric systems best meet its needs.

Law enforcement officers from as many as 18,000 separate state and local law enforcement agencies are estimated to fly armed. State and local law enforcement officers need only to present their agency's credential and a letter on the agency's letterhead stating that they have a work-related reason to fly armed. It has also been estimated that federal law enforcement officers from as many as 130 different agencies may fly armed even if they are not on official business. The number of different types of law enforcement credentials is a security problem for officials that must

[6] TSA, Registered Traveler: Our Approach, http://www.tsa.gov/approach/rt/index.shtm.

authenticate them, not to mention the proliferation of fake law enforcement credentials that are available on the Internet.

Along with biometrics usage for airport access control, the *IRTPA* required TSA to begin issuing a uniform biometric law enforcement credential within 120 days of enactment. Federal, state and local government law enforcement officers that want to fly armed present a TSA-issued credential that can biometrically authenticate their identity.

During a May 2004 Aviation Subcommittee hearing on the *Use of Biometrics in Aviation Security,* several witnesses and Subcommittee members urged the TSA to promulgate guidelines and standards for biometrics. The GAO also recommended that the TSA assess current access control technologies, including biometrics, and issue guidance regarding what technologies airports should use. Because the TSA had not issued any guidance, airports held off on equipping with biometrics systems. Airports do not want to purchase a system and then have the TSA require something else.

The *IRTPA* also mandated that the TSA issue guidance and operational requirements for biometrics systems by May 31, 2005. Though biometric technology is being tested at several airports (BOS, DEN, and San Francisco International Airport) across the country, TSA has yet to issue a uniform biometric law enforcement credential or guidance and operational requirements for biometrics.

II. Domestic Passenger Air Cargo[7]

The screening of passenger air cargo has long been an issue. Potential threats include: illegal shipments of hazardous materials; plots to place explosives aboard aircraft; criminal activities such as smuggling and theft; and potential hijackings and sabotage by persons with access to aircraft. Several procedural and technology-based initiatives to enhance air security and deter terrorist and criminal threats have been put in place or are under consideration. *ATSA* contains general provisions for cargo screening, inspection, and security measures. Under *ATSA*, cargo carried in passenger airplanes must be screened or its security otherwise ensured. In practice, TSA has relied heavily on "known shipper protocols"[8] to prevent shipments of cargo from unknown sources on passenger aircraft.[9]

The *IRTPA* included provisions establishing a pilot program for evaluating the deployment of blast-resistant cargo containers; promoting the research, development, and deployment of enhanced air security technology; evaluating international air threats; and finalizing operational regulations of air security. Those regulations require the use of an industry-wide known shipper database, background checks of workers, and enhanced security measures. In addition to these measures, Congress has provided appropriations to hire more canine teams and inspectors.

[7] In 2006, TSA finalized new rules for all-cargo flights that require the use of an industry-wide known shipper database, background checks of air cargo workers, and enhanced security measures at air cargo operations areas.

[8] Known shipper protocols include procedures for differentiating trusted shippers, known to a freight forwarder from unknown shippers, which then require additional screening and inspection.

[9] Bart Elias, *Aviation Security: Background and Policy Options for Screening and Securing Air Cargo*, Congressional Research Service (February 25, 2008) at 13.

The *9/11 Commission Act*, requires TSA to screen 50 percent of all cargo shipped on board passenger aircraft by February 2009, and 100 percent screening by August 2010. TSA Assistant Administrator John Sammon recently stated that through a combination of focusing on high-volume cargo airports and high-volume passenger flights, TSA expects to meet the 50 percent requirement in the Act.[10] The *9/11 Commission Act* also directs the TSA to implement a program for deploying blast-resistant cargo containers for use by air carriers on a risk-managed basis.

III. Secure Flight -- U.S. Visitor and Immigrant Status Indicator Technology (US-VISIT)

TSA created the Secure Flight program in response to the *IRTPA* and the *9/11 Commission Act,* which mandates that TSA assume the passenger pre-screening function from the airlines. Currently, airlines are responsible for matching passengers to the Terrorist Screening Center (TSC) watch list. According to TSA, Secure Flight[11] will increase the security of the TSC watch-list, improve screening consistency and efficiency.

On August 23, 2007, TSA published a notice of proposed rulemaking (NPRM) for implementing Secure Flight. Along with the Secure Flight NPRM, on August 23, 2007, TSA published a related but separate final rule regarding the Advance Passenger Information System (APIS) administered by U.S. Customs and Border Protection (CBP) for screening passengers of international flights departing from or arriving to the United States.[12] TSA states:

> We propose that, when the Secure Flight rule becomes final, aircraft operators would submit passenger information to DHS through a single DHS portal for both the Secure Flight and APIS programs. This would allow DHS to integrate the watch list matching component of APIS into Secure Flight, resulting in one DHS system responsible for watch-list matching for all aviation passengers.[13]

According to the August 23, 2007, Secure Flight NPRM, in accordance with the *IRTPA*, "TSA would receive passenger and certain non-traveler information, conduct watch-list matching against the No Fly and Selectee portions of the Federal Government's consolidated terrorist watch-list, and transmit boarding pass printing instructions back to aircraft operators."[14] TSA expects to assume watch-list matching for domestic flights beginning in January 2009 and to assume the function from the CBP for flights to and from the United States by FY 2010.

The DHS established the US-VISIT program to collect, maintain, and share data on selected foreign nationals entering and exiting the United States at air, sea and land ports of entry. This data includes biometric digital fingerprints to be used to screen persons against watch-lists, verify visitors' identities, and record arrival and departure. CBP officers use an inkless, digital finger scanner to capture finger scans of each person entering the United States.

[10] John Doyle, *TSA Claims Ability to Screen 50% of Cargo on Airlines by Feb. 2009,* Aviation Daily, July 16, 2008, at 2.

[11] TSA will not use Secure Flight to check for outstanding warrants, which was originally included in the program.

[12] Advance Electronic Transmission of Passenger and Crew Member Manifests for Commercial Aircraft and Vessels; 72 Fed. Reg. 48320, (August 23, 2007).

[13] Secure Flight Program; 72 Fed. Reg. 48356, (August 23, 2007).

[14] Ibid.

In May of 2007, DHS completed its biometric exit pilot program, which consisted of kiosks that collect inkless digital fingerprints. DHS found that the program technology worked, but that the program had low traveler compliance. The DHS determined that US-VISIT air exit procedures should be incorporated into the existing international visitor departure process to ensure seamless biometric collection regardless of the visitor's departure point. On April 24, 2008, DHS issued a NPRM[15] requiring commercial air carriers and vessel owners and operators to collect and transmit biometric exit information to DHS, in conjunction with passenger manifest information already being collected and submitted by the carriers. Air carriers are opposed to the rule because they consider the collection of biometric exit information to be inherently governmental. The proposed rule would not apply to small carriers and vessel owners and operators, or to general aviation.

IV. Foreign Repair Stations

The Federal Aviation Administration oversees the safety of repair stations but not the security of the facilities. To address the security oversight of facilities, Congress passed *Vision 100* (P.L. 108-176) in December 2003 and the *9/11 Commission Act*, both of which mandate that the TSA issue regulations to ensure the security of foreign and domestic repair stations certified by FAA, complete a security review, and audit of foreign repair stations certified by the FAA. Under the *9/11 Commission Act*, if the TSA does not issue a final rule by August 3, 2008, the FAA will be prohibited from issuing new certificates to foreign repair stations; there is an exception for certificate renewals and applications in process.

[15] Collection of Alien Biometric Data upon Exit from the United States at Air and Sea Ports of Departure; United States Visitor and Immigrant Status Indicator Technology Program; 73 Fed. Reg. 22065, (April 24, 2008).

WITNESSES

PANEL I

The Honorable Kip Hawley
Assistant Secretary
U.S. Department of Homeland Security
Transportation Security Administration

Ms. Cathleen A. Berrick
Director
Homeland Security and Justice Issues
U.S. Government Accountability Office

Panel II

Mr. Tim Campbell, A.A.E.
Executive Director
Maryland Aviation Administration
Baltimore/Washington International Thurgood Marshall Airport

Mr. Charles Barclay, A.A.E.
President
American Association of Airport Executives

Mr. John M. Meenan
Executive Vice President and Chief Operating Officer
Air Transport Association

Mr. Ajay Mehra
President
Rapiscan Systems, Inc.

Mr. Steven Brill
Chairman and Chief Executive Officer
Clear | Verified Identity Pass, Inc.

Captain John Prater
President
Airline Pilots Association, International