

Statement of
John S. Pistole
Administrator
Transportation Security Administration
U.S. Department of Homeland Security
Before the
United States House of Representatives
Committee on Homeland Security
Subcommittee on Transportation Security
June 2, 2011

Good afternoon Chairman Rogers, Ranking Member Jackson Lee, and distinguished Members of the Subcommittee. We appreciate the opportunity to appear before you today as the subcommittee begins consideration of a Transportation Security Administration (TSA) authorization bill.

TSA employs risk-based, intelligence-driven operations to prevent terrorist attacks and to reduce the vulnerability of the Nation's transportation system to terrorism. Our goal at all times is to maximize transportation security to stay ahead of the evolving terrorist threat while protecting passengers' privacy and facilitating the flow of legitimate commerce. TSA works collaboratively with industry partners to develop and implement programs that promote commerce while enhancing security and mitigating the risk to our Nation's transportation system. We also work closely with other federal agencies and maximize participation from state, local, tribal and private sector stakeholders to work toward a common goal of securing all modes of transportation, including aviation and surface transportation systems.

TSA has implemented an effective and dynamic security system in the aviation domain consisting of multiple layers of risk-based measures. In the aviation arena, our security approach begins well in advance of a traveler's arrival at an airport, with our vetting programs and intelligence analysts, cargo and compliance inspectors ensuring that airport security plans are

followed, and our law enforcement and intelligence community partners working to detect, deter, and prevent terrorist plots before they happen. The security system continues at the airport, including, but not limited to, the work of our Behavior Detection Officers (BDO); Transportation Security Officers (TSO) and the technology that supports the screening of passengers and baggage; Bomb Appraisal Officers (BAO); and canine teams, as well as our partnerships with local law enforcement. In flight, thousands of Federal Air Marshals (FAM) and Federal Flight Deck Officers (FFDO) protect the traveling public. The traveling public also plays an integral part role in the security system. For example, the DHS “If You See Something, Say Something” campaign engages the public and key frontline employees to identify and report indicators of terrorism, crime and other threats to the proper transportation and law enforcement authorities.

In the surface transportation arena, we continue to work with our law enforcement and security partners to reduce vulnerabilities and strengthen resilience against a terrorist attack. TSA works with the Federal Emergency Management Agency Grants Program Directorate to direct federal grants to the most at-risk transit properties. Our Surface Transportation Security Inspectors assist with the development of specific security programs. Our Visible Intermodal Prevention and Response (VIPR) teams are deployed on thousands of mass transit, pipeline, maritime and highway missions annually to enhance security, provide deterrent and detection capabilities, and introduce an element of unpredictability in security practices and procedures in order to prevent or disrupt potential terrorist planning activities.

TSA also conducts protection, response, detection, and assessment activities in airports and other transportation systems; trains and manages all armed pilots; and coordinates all TSA canine assets. Our personnel are continually adjusting and adapting security practices and procedures to best address evolving threats and vulnerabilities, and disrupt the ability of terrorists to plan and execute attacks.

TSA Security Operations and Technology Deployments

TSA works diligently to protect the U.S. transportation domain against evolving threats to security. We continue to modernize our technology, including Advanced Imaging Technology (AIT). We have deployed nearly 500 AIT machines at domestic airports throughout the country to enhance security by safely screening passengers for metallic and non-metallic weapons and

explosives – including objects concealed under layers of clothing, while protecting the privacy of the traveler. We will procure and deploy an additional 500 AIT units using FY 11 funds for a total of 1,000 AIT units, which will allow us to screen an estimated 60 percent of passengers using this technology. We have also deployed new portable explosive trace detection machines, Advanced Technology X-ray systems, and bottled liquid scanners to enhance our security technology in the aviation domain. This suite of technologies represents the most effective means of detecting current threats available today.

In order to continue the deployment of this critical layer of security, the President's FY 2012 budget request includes \$105.2 million in base and additional funding to deploy and staff 275 additional AIT units, bringing total coverage to 1,275 AITs by the end of 2012 and providing coverage to 80 percent of passengers. Congressional funding directly affects our ability to deploy this critical technology.

While we are rapidly deploying AIT machines to U.S. airports, we also are exploring enhancements to privacy protections and operational utility. Specifically, TSA has field tested auto-detection software for AIT machines, referred to as Automatic Target Recognition (ATR). ATR eliminates passenger-specific images of a passenger and instead highlights a detected anomaly on a generic outline of a person. Pat-downs used to resolve such anomalies are limited to the areas of the body displaying an alarm unless the number of anomalies detected requires a full-body pat down. If no anomalies are detected, the screen displays the word "OK" with no icon. With ATR, the screen will be located on the outside of the machine and can be viewed by the TSO and the passenger.

As with current AIT software, ATR-enabled units deployed at airports are not capable of storing or printing images. The ATR software eliminates the need for a TSO to view passenger images in a separate room because no visual image of the passenger is produced, reducing associated staffing and construction costs. ATR software represents a substantial step forward in addressing passenger privacy concerns, while maintaining TSA's standards for detection. TSA plans to continually update and test enhanced versions of the software in order to ensure that technology with the highest detection standards is in use.

In addition to deploying the most effective technology, we have also deployed additional BDOs, FAMs, and explosives-detection canine teams at airports throughout the country. We have implemented security measures for all air carriers with international flights to the U.S. that use real-time, threat-based intelligence to better mitigate the evolving terrorist threat. Last November, we achieved a major aviation security milestone: 100 percent of passengers on flights within, departing from, or bound for the United States are now checked by TSA against government watchlists through the Secure Flight Program, as recommended in the *9/11 Commission Report*. Continuous Secure Flight vetting begins 72 hours in advance of flight and continues until the flight departs, consistently providing insight into potential threats and enabling TSA and our law enforcement partners to counter these threats accordingly.

State Laws That Could Adversely Impact AIT Deployment

It is fitting that, as this Subcommittee considers new authorizing legislation for TSA, we address an issue that has recently received some media attention. Since the deployment of AIT and the implementation of our revised pat-down procedures at airport checkpoints nationwide to better detect prohibited items and resolve anomalies that are detected on passengers, some state legislatures have introduced legislation that would ban AIT units and even criminalize certain TSA pat-down procedures. It is TSA's position that, since TSA is a federal agency, individual states are preempted from interfering with the deployment of TSA personnel and equipment in carrying-out statutorily mandated security programs that are necessary to keep our aviation security system strong and safe for the traveling public. It is also important for our workforce to know TSA will stand by them as they execute their important responsibilities. State law proposals that would attempt to restrict cooperation between airport authorities and TSA in performing security measures diminish aviation security and leave the aviation system more vulnerable to a real and continuing terrorist threat.

Surface Transportation Security

TSA's efforts in the surface transportation domain are undertaken to reduce security vulnerabilities and to strengthen resilience against a terrorist attack. TSA works with its partners to secure and safeguard the surface transportation domain – which includes subways, bus transit systems, ferries, pipelines, the National Railroad Passenger Corporation (AMTRAK), commuter

railroads, and freight railroads, among others – through a variety of programs. Many of these programs enhance security by addressing policy gaps and obstacles, enhancing coordination and unity of effort, and maximizing the strengths and capabilities of our partners, keeping with the themes that guided the March 2010 Surface Transportation Security Priority Assessment.

Because mass transit and passenger rail systems serve large populations in major metropolitan areas, many with substantial underground infrastructure, bridges, and transportation staging areas, or hubs, which can include other forms of transportation, these systems remain a target for terrorist groups. The characteristics essential to mass transit and passenger rail – i.e., an inherently open architecture moving large populations in major metropolitan areas through multimodal systems and infrastructure – create potential security vulnerabilities. TSA uses a collaborative approach- working with state and local law enforcement and transit authorities- to assess risks and enhance security.

TSA’s role in surface transportation security involves direct engagement with surface transportation owners and operators to establish security standards, provide grant funding, share current risk information and assess security measures. For example, TSA uses the Transportation Systems Sector Risk Assessment to evaluate threat, vulnerability and consequence in a wide range of terrorist attack scenarios for each mode of transportation. To help address the results of these assessments, the Department of Homeland Security’s (DHS) Transit Security Grant Program (TSGP) provides awards to eligible transit agencies to assist state and local governments in devising and implementing initiatives to improve security. The TSGP promotes a sustainable, risk-based effort to protect critical surface transportation infrastructure and the traveling public from acts of terrorism. In 2011, DHS announced a new model for TSGP to focus limited resources on “shovel ready” projects hardening the highest-risk transit infrastructure, while prioritizing operational deterrence activities such as training, exercises, canine and mobile screening teams.

TSA also currently operates 25 VIPR teams across the transportation sector, and the FY 2012 budget request includes funding for 12 additional multi-modal VIPR teams. These teams consist of personnel with expertise in inspection, behavior detection, security screening, and law enforcement for random, unpredictable deployments throughout the transportation sector to deter

potential terrorist acts. There have been more than 3,000 VIPR operations in the current fiscal year, 70 percent of which occurred in the surface transportation sector.

In addition, structural vulnerability assessments are currently being conducted on the nation's most critical highway, bridge and tunnel infrastructure. These assessments, performed for TSA by the U.S. Army Corps of Engineers, are the most comprehensive assessments that have ever been performed. Additional assessment visits are also taking place at the state level and in conjunction with the companies that transport goods and passengers across the country. Finally, TSA is delivering security awareness training to the highway transport community; more than 200,000 individuals have been trained by the TSA-directed "First Observer™" program and similar TSA-sponsored training. Further, in response to a strong demand, TSA has distributed counterterrorism guides throughout the trucking, motor coach, school transportation, and infrastructure community.

Air Cargo Security

TSA has and will continue to focus air cargo resources to ensure continued compliance domestically with the 100 percent screening requirement, and to work toward further risk-based screening of international inbound air cargo on passenger and all-cargo aircraft. Along with its participation in the DHS Air Cargo Security Working Group established by Secretary Napolitano, TSA is continuing its leadership role in partnering with industry and other federal government partners to develop strategies to strengthen air cargo security while facilitating the flow of commerce. In January 2011, TSA issued proposed air carrier security program changes to increase security measures for air cargo, most notably, to require 100 percent screening for inbound international air cargo transported on passenger aircraft by the end of this calendar year. TSA is currently finalizing its analysis of industry comments. TSA is also working closely with U.S. Customs and Border Protection and the air cargo industry to receive and process pre-departure, advanced air cargo information about shippers earlier than is currently required so that we can increase the focus of our screening resources on high-threat cargo. TSA will also continue its efforts to test, evaluate, and qualify air cargo screening technologies.

TSA Explosive Detection Initiatives

TSA continually seeks to enhance capabilities for explosives detection as part of its risk-based and intelligence-driven strategy. To enhance our application and deployment of explosive detection canines, TSA partners with academic, research and professional organizations with the appropriate research capabilities to develop, explore and implement emerging explosive detection methodologies that have been subjected to extensive, rigorous research and testing. Further, TSA works with these organizations to determine how to harness these methodologies to gain the maximum explosives detection efficiency in the transportation system.

Last January, TSA, in partnership with the DHS Science and Technology Directorate, initiated a pilot program to evaluate 10 air scenting explosives detection canine teams, utilizing the methodology developed by Auburn University known as “vapor wake” explosives detection. The methodology relies on the canine’s ability to process air currents and recognize odors that it is trained to detect, whether the scent emanates from a person who is moving or standing still, or an inanimate object. Neither the canine nor the handler needs to come into direct physical contact with a person who may be a potential target – in fact, the canines can detect a scent even if the potential threat has left the immediate area and track the scent to its current location. A major advantage of this methodology is that the handler is trained to read the canine’s behavioral changes to determine when and where the canine is alerting to an explosives odor, on a subject, without the knowledge of the targeted subject.

A Risk-Based Strategy for the Future

TSA’s existing security measures create a multi-layered system of transportation security that mitigates risk. No layer on its own solves all our challenges, but, in combination, they create a strong and formidable system. In the months ahead, I am optimistic that we will be able to brief this Subcommittee and others in Congress about some initial steps we are taking to further enhance security by becoming even more risk-based in our approach to aviation security.

As our risk-based approach evolves, we must ensure that each new step we take strengthens security. Since the vast majority of the 628 million annual air travelers present little

to no risk of committing an act of terrorism, we should focus on those who present the greatest risk, thereby improving security and the travel experience for everyone else.

Since I became TSA Administrator a year ago, I have listened to ideas from people all over the world, from our dedicated workforce to our counterparts abroad, about how TSA can work better and smarter. Last fall I directed the agency to explore ways to develop a strategy for truly risk-based security. That strategy will examine the procedures and technologies we use, how specific security procedures are carried out, and how screening is conducted. While TSA currently implements a risk-based security system, we must continue to assess our programs to evolve our security approach to stay ahead of tomorrow's security threats.

To that end, we are working to expand our ability to conduct more identity-based screening. This is evident in our work on a new crewmember screening system. We are currently testing an identity-based system to enable TSA security officers to positively verify the identity and employment status of pilots. We hold pilots responsible for the safety of the traveling public every time they fly a plane. It just makes sense to treat them as trusted partners, as well.

While the initial iteration of this risk-based screening focuses on pilots, we are also looking at long-term concepts to focus limited resources on higher-risk passengers, while expediting and enhancing the passenger experience at the airports whenever possible. This will be an ongoing, collaborative effort with law enforcement, airport authorities and the traveling public. As our risk-based screening evolves, we will continue to incorporate random security steps as well as other measures both seen and unseen.

2011 Authorization Bill

As the Subcommittee considers a TSA authorization bill, two issues that deserve close consideration include the following:

Aviation Security Service Fee

Since its establishment in 2001 as part of the Aviation and Transportation Security Act, the Passenger Civil Aviation Security Service Fee has been limited to \$2.50 per passenger enplanement with a maximum fee of \$5.00 per one-way trip and has not been adjusted for inflation or the increased costs of providing security over the past nine years. Despite

Congress's original intent that the Security Fee cover nearly all costs related to passenger and property screening, the fee currently offsets less than a third of the total cost of aviation security. At the same time, costs of security have continued to increase. In FY 2010, the average cost for the TSA to screen a passenger and baggage was nearly \$9; in 2000, the cost was less than a dollar per passenger.

We ask that the Subcommittee give serious consideration to the President's Fiscal Year 2012 budget proposal to permit DHS/TSA to gradually increase the Passenger Civil Aviation Security Service Fee. This adjustment will ensure that we are able to continue the significant progress we have made in enhancing aviation security while fulfilling Congress' intent to do so in a fiscally responsible manner that does not penalize American taxpayers.

Procuring and Installing EDS Equipment with ASCF Funding

As you know, current law requires the first \$250 million derived from passenger and air carrier security fees in Fiscal Years 2004 through 2028 to be deposited in an Aviation Security Capital Fund (ASCF).

The ASCF is distributed to airports through grants for airport security capital improvement projects. These projects typically include facility modifications, design and build-out for integrated baggage handling and Explosives Detection Systems (EDS). These grants cannot be used for the procurement and installation of the actual explosives detection equipment that these modifications are designed to accommodate, however, because TSA, and not the airports who receive these grants, is responsible for the procurement and installation of that equipment.

TSA has already funded, or is currently funding, most of the projects eligible for ASCF funding and does not expect applications for many new eligible projects in the foreseeable future. A critical need exists, on the other hand, for TSA to procure and install large quantities of the EDS equipment itself, in order to replace aging and less up-to-date security technologies. TSA currently has approximately 2000 EDS units deployed nationwide. By 2013, almost half of those units will have reached the end of the anticipated useful life of 10 years. Because the EDS equipment is an integral part of the projects Congress intended to fund with the ASCF, we ask

this Subcommittee to give serious consideration to correcting this situation by adopting a provision to permit the ASCF to be used for the procurement and installation of EDS equipment.

Additionally, current law requires TSA to issue letters of intent (LOI), which are agreements to provide funding over a period of several years. Again, the major projects for which such funding would be appropriate have already been funded. On the other hand, there is a need to fund smaller capital projects through single-year funding. We request this Subcommittee consider amending the law to permit use of the ASCF in this manner. With these two amendments to the ASCF language, TSA could more effectively, efficiently, and expeditiously plan and implement the necessary acquisition and replacement of existing EDS units, and provide funding to airports for smaller capital aviation security projects that do not require multi-year funding.

Conclusion

I want to thank the subcommittee for its continued assistance to TSA and for the opportunity to discuss our programs as the subcommittee initiates its work on a TSA authorization bill. I am pleased to answer any questions you might have.