

DEPARTMENT OF HOMELAND SECURITY  
STATEMENT OF ADMIRAL JAMES M. LOY  
ADMINISTRATOR, TRANSPORTATION SECURITY ADMINISTRATION  
ON TRANSPORTATION SECURITY  
BEFORE THE  
COMMITTEE ON TRANSPORTATION AND INFRASTRUCTURE  
SUBCOMMITTEE ON AVIATION  
UNITED STATES HOUSE OF REPRESENTATIVES  
October 16, 2003

Good morning Mr. Chairman, Congressman DeFazio, and Members of the Subcommittee. I am pleased to have this opportunity to appear before you today to report on the Transportation Security Administration's (TSA) progress and plans for improving security in the Nation's aviation transportation system.

Under the leadership of Secretary Ridge and Under Secretary Hutchinson, we have forged working partnerships with other Department of Homeland Security (DHS) organizations, and we continue to work closely with the Federal Aviation Administration (FAA) of the Department of Transportation (DOT). They provide another vital link with air carriers, airport operators and aviation associations, and we communicate daily to share expertise to ensure that we make the best use of each organization's resources and opportunities.

Much has been accomplished in less than two years since enactment of the Aviation and Transportation Security Act (ATSA), and less than one year since completion of the federalization of passenger security screening at U.S. airports. I feel confident in assuring you and the American people that the civil aviation sector is more secure today than it has ever been, but I am mindful that as a young organization there is much yet to be done, as we mature our many-layered "system of systems." Today, I would like to focus on the performance of TSA screeners—a critical line of defense in the multiple rings of security that comprise our system of systems approach to aviation security. As our system of systems approach recognizes that no human workforce alone, no matter how skilled, well-trained, and well-supervised, can assure absolute security, I will also review briefly some of the other major strides that we have made in aviation security that complement the work of our screeners, and our action plan for making further improvements.

Every passenger entering the sterile areas of an airport is screened by members of a highly trained force of TSA screeners.<sup>1</sup> National, validated skill standards for all screeners form the foundation for an integrated system for hiring, training, certifying, and measuring performance. Our screeners must meet national standards that demonstrate qualifications, knowledge, skills, and aptitudes necessary to successfully perform as a

---

<sup>1</sup> TSA is also operating a pilot program at five airports using private screeners that must meet all TSA eligibility, training, and performance requirements and must receive pay and other benefits equal to those of TSA screeners.

transportation security screener. They receive a minimum of 40 hours of classroom training, and 60 hours of on-the-job training. Screeners are subject to periodic proficiency assessments and unannounced testing. They are made aware of new threats and methods of concealment. This stands in marked contrast to the workforce responsible for U.S. airport security screening before the creation of TSA. Screeners employed by the airlines, often through contracts with private companies, received minimal training and were often poorly motivated. Contract screening forces were plagued with high rates of attrition that resulted in an average screener tenure of 4.5 months, making it all but impossible to develop the consistent level of proficiency required to assure reliable screening.

No matter how qualified a screening workforce is, maintaining a high level of screener proficiency requires constant vigilance. We have a multi-layered approach to monitoring and improving performance. On the most basic level is the initial training. Screeners who fail any operational test must complete remedial training as a condition of continuing with their screening duties. A recurrent training program is under development; two modules have already been delivered to the field, and Federal Security Directors (FSDs) have been encouraged to use the training modules of the Basic Screener Course as recurrent training. Many have done so and others have developed their own supplementary training. Additionally, screeners are required to undergo weekly x-ray image interpretation training using state-of-the-art computer-based training. Our personnel at airports have received the first of a series of screener performance improvement videos, and will have access to more than 350 courses via the new Online Learning Center that goes live this month or via compact discs. We are also certifying over 800 screeners and training coordinators to teach various topics at each airport.

Finally, approximately 500 of our 3600 screener supervisors have been enrolled in a U.S. Department of Agriculture (USDA) Graduate School Introduction to Supervision course through September. This month the course is being modified to be airport security specific, and starting in November the course will be further tailored to meet the needs of screening supervisors, and will be offered beginning in March, 2004. An advanced course for screener supervisors to provide them with a higher level of technical knowledge and skills is also being developed.

All screeners must meet annual recertification standards, which require passenger screeners to pass an Image Certification Test, SOP (standard operating procedures) Job Knowledge Test, and Practical Skills Demonstration, and requires checked baggage screeners to pass an SOP Job Knowledge Test and Practical Skills Demonstration. In addition to passing these tests, developed at the national level, FSDs will be responsible for ensuring that all screeners have a satisfactory record of performance in accordance with their individual performance management plan. Recertification for 2003-04 began on October 1, 2003, and will run through approximately March 2004. As part of our recent rightsizing effort, approximately 28,000 screeners completed proficiency testing; we will consider successful completion of those tests to be a part of the annual recertification.

In July of this year we conducted a Screener Performance Improvement Study to determine the root causes for deficiencies in screener performance. After identifying what the desired level of screener performance should be, we gathered data from multiple sources to determine the actual, current level of performance and the root causes of the gap between desired and actual performance. Based upon this study, we have identified an array of solutions and are in the process of evaluating and implementing them. Some solutions are focused on additional training, as already discussed; however, those solutions are dependent upon providing network connectivity to training computers to afford access to real-time training on current threats.

We are also in the process of implementing an updated version of the Threat Image Projection System (TIP), originally deployed by FAA after operational evaluation and validation testing in 1999. TIP is a system that superimposes threat images on x-ray screens during actual operations and records whether screeners identify the threat object. By frequently exposing screeners to images of a variety of dangerous objects, the system provides continuous on the job training and immediate feedback and remediation, and allows supervisors to monitor screener performance.

Our TIP system is already greatly improved over the FAA system in several respects. First, we are expediting the replacement of the approximately 1,800 conventional x-ray machines with TIP-ready x-ray machines (TRXs). We now have over 1,300 new TRXs in place. Additionally, whereas the FAA used a library of only a few hundred images, which were frequently shared with screeners, eliminating any real test value, we are deploying a more comprehensive library of 2,400 images. We expect the new TSA TIP image library to be deployed on all TRX machines that are in place by the end of this calendar year. Through the combination of increased deployment of TRX machines and deployment of the expanded TIP image library, we will be able to collect and analyze significant amounts of performance data that had not been previously available to us. As we continue to deploy the expanded TIP library on all TRXs, during the months of October and November, we will primarily rely on using the limited library as an on-going training tool and to provide limited, local performance data to FSDs. Once TSA has the expanded TIP library on all TRXs in place (end of November), we will collect and analyze the data in December, allowing us to establish our first, national baseline view of screener performance, as measured by TIP, using the fully expanded TIP library of 2,400 images. This baseline view will help us better understand our strengths and weaknesses, allowing us to implement appropriate skill enhancement strategies. Finally, although the FAA collected TIP data and published it occasionally, for technical reasons the data was never used in any meaningful way for improving screener performance as planned in the early stages of development. In contrast, we will be using TIP as it was intended--an active training and management tool, used to evaluate individual screener skills and enable us to focus on areas needing skill development.

Yet, training alone is not sufficient to sustain excellence. Another important tool is our operational testing program, which consists of unannounced, covert testing at airports

across the nation, as required by law,<sup>2</sup> performed by a select professional staff. Through this program, we challenge screeners to detect threat objects at screening checkpoints and in checked baggage, using simulated terrorist threat devices and current techniques. Timely feedback on the results of these tests is provided to screeners, FSDs, and other TSA officials to drive change and improvement through modification of our SOPs, remedial training, or improving technology, as appropriate. The covert tests serve as one of many indicators of screener performance, and must be viewed in the context of a larger performance measurement system, that includes individual screener TIP data, annual screener certification, supervisory oversight, the adequacy of our SOPs, and the reliability of equipment and technology. Between September 2002 and August 2003 our Office of Internal Affairs and Program Review (OIAPR) conducted 733 checkpoint tests and nearly 2,200 airport security access and checked baggage tests at 95 airports. We are conducting covert testing at over three times the annual rate of the old FAA “red teams,” and our testing uses more difficult, realistic testing situations. I cannot discuss the results of our tests in detail in this setting, because of the security sensitivity of the data, but I can say that generally results have shown an improvement of over 10 percent since testing began. This is particularly significant because the difficulty of the tests has increased over the past year. OIAPR’s testing plan is designed to test all airports during a three year period with Category X airports tested annually, Category I and II airports tested biannually, and contract screener pilot airports tested semiannually. The U.S. General Accounting Office (GAO) published a report in September 2003 of its preliminary observations on progress made in airport passenger screening, which was based in part upon their own covert tests and tests performed by the DHS Office of the Inspector General (OIG), in addition to the OIAPR tests. This report notes the continuing need to improve screener performance. We concur with that finding.

In sum, in this first year of a federalized screening force we have seen significant improvement over the pre-9/11 non-Federal screener performance, but we recognize we must constantly strive for an optimum level of performance. We are committed to continuous testing of the system and will constantly raise the bar on the difficulty and complexity of our testing to drive enhanced performance.

Our rightsizing effort continues as we work to find the balance between airport and air carrier needs, and staffing requirements for TSA passenger and baggage screeners to maintain effective security. After we ramped up to meet the deadlines for federalizing passenger and baggage screening, we had learned much about our staffing requirements. As we analyzed our staffing model, it was clear that there were airports where we had an imbalance in staffing at passenger screening checkpoints. In some airports this meant we had too many screeners for the passenger load at those locations. At others, particularly those in large metropolitan areas, we had too few screeners. In many locations it became clear that a part-time workforce segment makes sense, given the peaks and valleys of scheduled air carrier service. As a result, and in response to Congressional direction in connection with the FY03 appropriation, I made a decision to reduce the number of screeners by 3,000 by May 31, 2003, and by an additional 3,000 by September 30th of this year. We have reached these targets. Where we required additional part-time

---

<sup>2</sup> Title 49 U.S. Code §44916(b) and §44935(f)(6)

staffing at airports, we have begun to open assessment centers for individuals to apply for those positions.

In light of the fact that TSA met this difficult goal of reducing the workforce by 6,000 screeners before the end of this fiscal year, I ask this Committee's understanding of our need to pause and stabilize the screener workforce during the next 3 to 6 months. This will permit TSA to complete the conversion process of many screeners from full-time to part-time status as we re-shape the workforce. It will also allow us to complete the immediate requirements to hire additional part-time employees to maintain our current screener workforce levels and to balance the full-time equivalence (FTE) allocations at the various airports throughout the country.

Of course, even optimum human performance alone cannot get the job done completely. We have also greatly improved the technology used at screening checkpoints and have improved our capability to detect weapons, explosives, and other prohibited items. The combination of our screening force and enhanced technology has resulted in almost 800 arrests at screening checkpoints and the interception of over 4 million prohibited items since the November 19, 2002, deadline to have TSA screeners at all commercial airports.

During the past several months, the media has reported on improvised explosive devices secreted in ordinary items that passengers might carry onto an airplane, and continued attempts by terrorists to perfect the shoe bomb apparatus employed, unsuccessfully, by convicted terrorist Richard Reid in December, 2001. These threats are a stark reminder that we must maintain our focus on security through reasonable and prudent, but effective measures efficiently applied. The number of prohibited items that TSA screeners continue to intercept from passengers is still large. In June, July, and August of this year the number of weapons, explosives, and other prohibited items that our screeners intercepted totaled 1,436,969, a 28% increase over the number of prohibited items intercepted in the same time period in 2002, even though we have reduced the list of prohibited items to eliminate non-lethal items such as nail clippers. Among the items recently intercepted were a knife concealed inside a sealed soda can and a gun secreted in a child's teddy bear.

Although ATSA mandated the federalization of airport security screening, it held open the possibility that airports could return to contract screening, provided the high standards required of the Federal screening system could be met. TSA is currently operating a pilot program at five airports using private screeners that, by law, must meet all TSA eligibility, training, and performance requirements and must receive pay and other benefits equal to those of TSA screeners.

Beginning on November 19, 2004, any airport operator may apply to have screening performed by a contract screening company under contract with TSA. In preparation for this option, on September 26, 2003, we awarded a contract to perform a rigorous comparison of the performance of pilot program screeners with that of Federal screeners, to determine the reasons for any differences, and to develop criteria for permitting airports to opt out of the Federal screening program.

Many other elements in our system of systems complement our screening efforts. First, the flow of intelligence on terrorists, their methods and their plans, has greatly improved our understanding of the threats that we face and helped us focus our resources on meeting those threats. There have been countless times when information shared with airports or airlines has alerted them to threats and encouraged enhanced security on their part. In FY03 we issued 36 Security Directives (SDs) and 13 Emergency Amendments (EAs), and 26 Information Circulars (ICs)—16 of those in aviation.

TSA has increased cooperation with our international partners at airports overseas and with air carriers that fly into and out of the United States. We have required thousands of criminal history records checks for U.S. airport workers needing unescorted access to secure areas of the airport and we are working on improving the access process as part of our overall airport security program.

TSA and the FAA have helped fund many local airport projects to improve perimeter security, such as construction of perimeter access roads, installation of access control systems, electronic surveillance and intrusion detection systems, and security fencing. One local initiative demonstrates how quickly interagency cooperation can be marshaled to fill security gaps when they are discovered. When perimeter security was breached at New York's JFK Airport, the Port Authority of New York and New Jersey rapidly orchestrated an effective plan to enhance the protection of the remote runways of their facility.<sup>3</sup> A new level of perimeter security is now in place that involves people, technology, and innovation. It is also an example of the products that skilled security planners can develop locally, without specific direction from a Federal agency. Our own TSA security inspectors, FAA's Air Traffic Service, the Port Authority Police, the NYPD Boat Patrol, and the U.S. Coast Guard have joined forces to create a cooperative arrangement that will result in tighter perimeter security including the waterside runways of that airport.

The realization of and the response to the threat from Man Portable Air Defense Systems (MANPADS) is part of our focus on improved perimeter security, an element of the security plan required for each airport. We take the threat of MANPADS extremely seriously and continue to perform vulnerability assessments on our airports even as both the Science and Technology Directorate of DHS,<sup>4</sup> and the Department of Defense accelerate their review of technology to find the right way to protect commercial airliners from this threat. Other components to protect civil aviation from MANPADS include non-proliferation efforts and border and customs enforcement, all key areas that DHS, the State Department, the Defense Department, and many other agencies continue to pursue.

---

<sup>3</sup> Among the new measures that the Port Authority has instituted are increased perimeter patrols, posting police or security guards in marked patrol cars in unfenced boundary areas during nighttime hours, and directing other mobile patrol units to regularly monitor perimeter activity.

<sup>4</sup> The Science and Technology Directorate has issued a pre-solicitation notice as the first step in DHS's two-year \$100 million program to protect aircraft from shoulder-fired missiles. The two-phase systems development and demonstration program for anti-missile devices for commercial aircraft first, will analyze economic, manufacturing and maintenance issues to support a system that will be effective in a commercial aviation environment, and second, will include the development of prototypes using existing technology.

I want to emphasize, however, that there is no credible intelligence that MANPADS are in the hands of terrorists in this country.

As you know, we expanded the Federal Air Marshal Service (FAMS) from dozens of agents before 9/11 to thousands of highly trained law enforcement officers, flying the skies on both domestic and international flights. The FAMS will be transferred to the Bureau of Immigration and Customs Enforcement (BICE) no sooner than November 1, 60 days after notification was provided to Congress, as required by the Homeland Security Act. This will create a “surge capacity” to effectively support overall homeland security efforts by cross-training FAMS and BICE agents to counter aviation security threats.

Under FAA rules, all commercial passenger aircraft that fly in the United States now have reinforced cockpit doors, making it highly unlikely that terrorists could successfully storm the cockpit.<sup>5</sup> The “Crew Training Common Strategy” (commonly referred to as the “Common Strategy”), was originally developed by FAA to address hijacking threats. It was restructured immediately after 9/11, and TSA and FAA are currently engaged in a further revision to the Common Strategy to address the threats posed by suicide terrorists. Pilots are now trained to refrain from opening the flight deck door, and if terrorists should somehow breach the reinforced flight deck door, they would meet with a flight deck crew determined to protect the flight deck at all costs. An increasing number of pilots are armed and trained to use lethal force against an intruder on the flight deck.

We have implemented the Federal Flight Deck Officer (FFDO) program. We held the first training class this past April and we trained, deputized, and deployed our first group of volunteer pilots serving as Federal Flight Deck Officers. We closely reevaluated the training, and indeed, the entire program, and we have revamped both. In close cooperation with organizations representing many airline pilots such as the Air Line Pilots Association (ALPA) and the Coalition of Airline Pilots Associations (CAPA), we have begun full-scale training of volunteer pilots. The FFDOs that are currently flying have now flown over ten thousand flights, quietly providing another layer of security in our system of systems. As more FFDOs are deputized, this number will rise quickly into the hundreds of thousands of flights.

We transferred FFDO training on September 8, 2003, from the Federal Law Enforcement Training Center (FLETC) at Glynco, Georgia, to the new permanent site at FLETC’s training facility in Artesia, New Mexico. FLETC Glynco was operating over capacity, largely as a result of the added requirements for law enforcement training following September 11. The Artesia facility offers the capability to double the student throughput each week and we plan to do so starting in January 2004. FLETC Artesia is also the home of the basic training program of the FAMS, and thus, has training facilities specifically geared to the unique environment and circumstances present on an aircraft. FLETC Artesia has three environmentally controlled commercial passenger jets on

---

<sup>5</sup> In a widely reported statement, a spokesman for The Boeing Company, which has produced thousands of flight deck door conversion kits, related that the new door withstands bullets and small explosives and can resist a force equivalent to an NFL linebacker hitting it at Olympic sprinter speed.

hardstands available for use as tactical training simulators, and ample indoor and outdoor shooting ranges. Prior to starting our training in Artesia, a delegation of pilots and TSA staff visited the site and was unanimous in its praise of Artesia as a better option. I intend to use geographically dispersed facilities for semi-annual recertification training required of FFDOs, including private facilities. By the end of FY04, at the current pilot application rate, we expect to have trained the vast majority of pilots who have volunteered for the program and met the initial background requirements.

Over the last three months, I have been able to sign the first Letters of Intent (LOIs) that TSA has issued to airports. These LOIs will provide for the installation of explosives detection systems (EDS) that are integrated with efficient checked baggage handling systems, thus reducing unacceptable clutter in the terminal buildings. Integrated baggage systems foster efficient movement of passengers through the screening checkpoint while their checked baggage is screened by EDS and moves through the conveyor systems. TSA has established and is applying prioritization criteria to allocate appropriated funds amongst airports through the LOI program. I issued the first series of three LOIs to Dallas–Fort Worth International Airport, Boston–Logan International Airport and Seattle–Tacoma International Airport. I awarded another set of three LOIs for McCarran International Airport in Las Vegas, Denver International Airport, and Los Angeles International Airport and Ontario International Airport in California. These six LOIs, covering seven airports, represent a Federal commitment of approximately \$670 million over the next four budget cycles.

We know that we cannot solve all security concerns solely with the power of a strong security workforce. We must be able to develop and deploy new technology to make our screening operations more effective, more efficient, less time consuming, and less costly, and we must be able to look beyond the horizon to identify and adapt to emerging threats. Led in large part by our Transportation Security Laboratory (TSL), TSA is attempting to do just that.

The certification, purchase, and installation of some 1,000 explosives detection systems (EDS) and 5,300 explosives trace detection (ETD) machines at more than 400 airports throughout the country in such a short time after TSA was created met an aggressive congressional deadline. We are continuing to work on identifying the next generation of explosives detection equipment for use in screening carry-on and checked baggage. We are working with the vendors of the currently deployed technology to develop enhancements to existing EDS platforms to improve alarm rates, throughput and reliability. We are simultaneously working with new vendors to develop technologies that will enable us to detect explosives at lesser amounts than are currently established in our certification standard, and occupying a smaller footprint at already overcrowded airports. TSL is looking at new applications of X-ray, electro-magnetic, and nuclear technologies to better probe sealed containers for materials that pose a threat.

To help our screeners better identify explosives and weapons that an individual may attempt to carry into the cabin of an aircraft, we are testing two explosives trace detection portals that analyze the air for explosives as passengers pass through them. TSA has also

established a new performance standard for walk through metal detectors (WTMD) and replaced every WTMD at all U.S. commercial airports with the latest technology for these devices. We are developing a document scanner that will detect traces of explosives on a boarding pass type document handled by a passenger. We are also evaluating “body scan” technologies, such as backscatter x-ray, millimeter wave energy analysis, and terahertz wave technology.

We are replacing all checkpoint x-ray equipment with units that will be equipped with TIP to support the efforts previously mentioned for improving screener performance. We are also developing a system to multiplex TIP-ready x-ray units to allow more flexibility regarding staffing to monitor checkpoint operations. Our goal at the passenger screening checkpoint is to work towards sensor fusion, which will result in fewer boxes with combined capabilities.

I know that this Committee is very interested in blast resistant cargo containers that hold either cargo or luggage and contain an explosion. The issues we face with devices now available in the marketplace involve weight, cost, and durability. TSA, through TSL, is working on improving this technology for use on wide body aircraft by conducting explosive testing in a pressurized wide body aircraft to determine post-detonation survivability under simulated live conditions. We continue to need the airline industry’s assistance for hardened container operational evaluation and reliability testing.

Cargo security on passenger aircraft remains a matter of concern for this Committee and for all of us engaged in transportation security. I am firmly convinced that our air cargo security strategic plan is on the right track. Proposals to require the physical inspection of every piece of cargo shipped on passenger aircraft without a risk-based targeting strategy are no more practical than similar calls to physically inspect each of the more than 6 million containers that enter the United States each year through our seaports. Proposals of this sort would simply prevent any cargo from being carried on-board passenger aircraft. Rather, we have focused our efforts on three key components in ensuring the security of air cargo.

First, we use a threat-based, risk-management approach. All cargo manifests and other information should be screened for a determination of the threat and the risk that it poses. Certain cargo deemed suspicious or “high-risk” will be subjected to more intense security screening under the TSA approach. Part of this process involves banning cargo from unknown shippers from passenger aircraft, and greatly strengthening the “Known Shipper” program. Participation in the Known Shipper program is now more rigorous. Passenger air carriers, all-cargo carriers, and freight forwarders have been given added responsibility for verifying a customer’s status in the Known Shipper Program. TSA performs inspections of these links in the supply chain to ensure compliance. TSA is also moving forward with the Known Shipper Database and automated Indirect Air Carrier certification/recertification. TSA plans on the full deployment of this database in FY 04.

The second component of our strategic approach to air cargo security involves the use of information analysis to assist in “pre-screening” cargo. Using sources external to TSA,

we will gather information on whether or not cargo is of a suspicious origin, warranting additional scrutiny. TSA is already working with the Bureau of Customs and Border Protection (BCBP) and its National Targeting Center in the development of tools for pre-screening air cargo. Again, we plan to develop and begin deployment of our targeting efforts in FY 04.

The third component in our air cargo security strategic plan involves the development of technology to aid in screening and inspecting air cargo. Our goal is to subject higher-risk shipments to heightened security screening, but TSA will need a toolbox of inspection methodologies and technologies, as no one technology or technique can be applied in all operating environments. A combination of EDS, ETD, x-ray devices, and canine explosives detection teams, and perhaps even emerging technologies will need to be made available to the field. We will have to overcome a number of hurdles to be able to inspect cargo efficiently by remote means without damaging the contents or unnecessarily delaying shipment, and we will need to establish standards for detection and cargo facility design that reflect new security requirements. This research and development and deployment effort must be supported.

Air cargo security, just like security for all other aspects of the transportation system, is a partnership. The air cargo industry must participate with us in a collaborative effort and must be able to bear its fair share of the costs. I am grateful for the cooperation that TSA has received from the industry through its participation in cargo working groups, an offshoot of the Aviation Security Advisory Committee (ASAC).<sup>6</sup> On October 1, we received almost 40 recommendations from these groups, covering twenty-two topic areas, including enhancements to Known Shipper program, the development of additional screening technologies, greater security of Indirect Air carriers (freight forwarders), and enhanced security measures for the all-cargo air carriers. TSA will review these recommendations as part of the development of a strengthened regulatory program.

Our continuing efforts to improve aviation security inevitably focus on more accurate information about people who have access to various aspects of the aviation and overall transportation system. I am pleased with the continued support from the Congress for our Transportation Worker Identification Credential (TWIC) program. This program is developing a system-wide uniform credentialing standard which, if necessary, has the potential to be used across transportation modes for personnel requiring unescorted physical and/or logical access to secure areas of the transportation system. We believe that uniform credentialing standards will enhance security and make economic sense to an industry for which multiple cards and mixed standards are commonplace. Using funds already appropriated by Congress, we now have a technology evaluation underway in two regions. One is on the East Coast covering the Philadelphia-Delaware River area and the other is on the West Coast in the Los Angeles and Long Beach area of California.

---

<sup>6</sup> The Aviation Security Advisory Committee (ASAC) is a standing committee composed of federal and private sector organizations that was created in 1989 in the wake of the bombing of Pan Am 103 over Lockerbie, Scotland. In May 2003, three working groups of ASAC met for the first time to develop recommendations to the TSA to enhance cargo security.

The information that we glean from these technology evaluations will enable us to make key decisions about further development of this program.

Of course, our most visible mission since September 11<sup>th</sup> has been to keep terrorists off commercial airliners. Our plan to move forward with development, testing, and implementation of the second-generation Computer Assisted Passenger Prescreening System (CAPPS II) is critical to a robust aviation security system. As part of its ongoing dialogue with the public on CAPPS II and related issues, DHS has issued a revised Interim Final Privacy Notice, which provides information regarding CAPPS II, including the type of data that the system will review, and how the data will be used. As always, public comment on the Notice was requested. The closing date for submission of comments was September 30<sup>th</sup>. CAPPS II will be a threat-based system under the direct control of the Federal Government and will represent a major improvement over the decentralized, airline-controlled system currently in place. Mr. Chairman, I pledge to continue to work with this Committee to assure you and the Members of this Subcommittee that our development of CAPPS II will enhance security without compromising important privacy rights or our civil liberties.

We are also developing the parameters for a pilot program to test key elements of the voluntary "Registered Traveler" program, including background checks, positive identification, and new checkpoint operations. We intend to test these concepts at several airports later this year. Our airline partners have expressed strong interest in working with us.

TSA's actions to enhance aviation security are not limited to commercial aviation. We have made great strides in the last two years in improving security for the general aviation (GA) community. This is a substantial undertaking, as there are approximately 220,000 GA aircraft in the United States, responsible for 77% of all air traffic, and more than 18,000 landing areas throughout the nation. TSA has several initiatives underway that will continue to improve security in this critical arena. We are working collaboratively with key stakeholders in the GA community to develop and disseminate appropriate security guidelines for the thousands of public and private use GA airports and heliports. TSA is conducting detailed planning in preparation for launch of a GA vulnerability assessment in early 2004. Coordination with the Directorate for Information Analysis and Infrastructure Protection (IAIP) is ongoing to ensure that this assessment is harmonized with the overall DHS risk management program. We are looking at more in-depth background checks for some GA pilots. This would assist in issuing waivers to certain restricted airspace to cleared individuals such as corporate pilots. Finally, we are reviewing with the FAA and other agencies some of the restrictions in current FAA Notices to Airmen (NOTAM) to assess their security value. We will advise the FAA about whether certain airspace restrictions add real security value and we will recommend that FAA engage in appropriate rulemaking to permanently codify those security-based airspace restrictions that add real security value.

In conclusion, during these two years since the tragic events of 9/11, we have come a long way in meeting the enormous challenges presented to us in the Nation's call to

improve the aviation security system. We have built a highly skilled screening force and have worked diligently to assure that imbalances in the initial placement of screeners in airports across the Nation are corrected by staffing adjustments. We have enhanced security technology at airports across the nation and expect to have electronic screening for explosives of all checked baggage in all but five airports by December 31, 2003. We have all learned a great deal very quickly, and will continue to do so as we refine our training and testing methodologies, always striving to use every tool at our disposal to motivate our screeners and drive our entire screening system toward excellence.

We can surmount the very real threats to our security only by working as a team. You have my assurance that TSA will continue to reach out to all elements of the aviation transportation and security communities, public and private, as we move forward. Our goal remains reasonable and effective security, efficiently applied. Thank you for the opportunity to testify before you today. I will be happy to answer any questions you may have.