

U.S. DEPARTMENT OF HOMELAND SECURITY
TRANSPORTATION SECURITY ADMINISTRATION
STATEMENT OF STEPHEN J. McHALE
DEPUTY ADMINISTRATOR
ON TRANSPORTATION SECURITY

Before the
SUBCOMMITTEE ON INFRASTRUCTURE AND BORDER SECURITY
SELECT COMMITTEE ON HOMELAND SECURITY

May 12, 2004

Good morning Mr. Chairman, Congresswoman Sanchez, and Members of the Subcommittee. I am pleased to testify before the Subcommittee on the progress of the Transportation Security Administration (TSA) in fulfilling its critical responsibilities to protect the Nation's transportation systems to ensure freedom of movement for people and commerce. I look forward to highlighting many of the significant advances TSA has made in the two years since the agency was established and since joining the Department of Homeland Security (DHS).

At TSA, we are designing a security strategy for a broader spectrum of responsibilities than we considered in the pre-9/11 world, ranging from enhanced awareness and information sharing, through prevention, protection, response, consequence management, and recovery. DHS was created to lead the unified national effort to secure America. The creation of DHS has produced a force multiplier and a vast network for awareness and information sharing to protect our Nation. Working under the guidance of the Border and Transportation Security Directorate (BTS), TSA's mission is completely aligned with the mission and goals of BTS and DHS. TSA collaborates extensively with other BTS agencies and with DHS components, such as the Science and Technology Directorate (S&T), the Information Analysis and Infrastructure Protection Directorate (IAIP), and the U.S. Coast Guard (CG), identifying opportunities to share information, resources, and expertise. We also continue to work closely with the Department of Transportation (DOT) and the modal administrations. They provide another vital link with transportation providers, and we communicate daily to share expertise and to ensure that we make the best use of each organization's resources and opportunities.

TSA continues to work to improve coordination with our sister agencies within DHS, as well as with our other Federal partners. In this regard, President Bush issued Homeland Security Presidential Directive 7 (HSPD-7) on December 17, 2003, which directs the establishment of "a national policy for Federal departments and agencies to identify and prioritize United States critical infrastructure and key resources and to protect them from terrorist attacks." HSPD 7 sets the framework for DHS to develop a National Critical

Infrastructure Protection Plan, and TSA has been specifically delegated the responsibility to develop the Sector Specific Plan (SSP) for Transportation under the National plan. The development of this plan will involve intensive interaction with other DHS directorates and agencies, such as IAIP and CG, in addition to DOT. The plan, which will be developed over the next several months will: (1) identify participants in the sector, their roles and relationships, and their means of communication; (2) identify assets in the sector; (3) assess vulnerabilities and prioritize assets in the sector; (4) identify protective programs; (5) measure performance; and (6) prioritize research and development.

To ensure security in each mode of transportation at an operational level, TSA is also working with our federal and other partners on the development of Modal Security Plans for each mode of transportation. We will expand the Transportation SSP to include modally-specific annexes that provide security planning guidance to modal security plan writers and industry stakeholders, and explicit links to the other National plans such as the National Response Plan (NRP) and the National Incident Management System (NIMS). On behalf of DHS and in conjunction with other federal agencies, the completed Transportation SSP will guide and integrate a family of transportation modal security plans to prevent, mitigate, and respond to intentional disruption of the Nation's transportation systems while ensuring freedom of movement for people and commerce.

The tragic bombings that occurred in Madrid on March 11 and in Moscow on February 6 were terrible reminders of the risk of terrorism to rail transportation. To that end, DHS, in conjunction with DOT, continually ascertains the threats, probabilities, and consequences of potential attacks on rail and other transportation systems using a risk-management approach. Effective strategic threat-based planning results from an evaluation of all available intelligence and an assessment of criticality and vulnerability information to determine the overall risk environment.

Domain awareness is the essential starting point of our overall transportation security strategy. TSA receives intelligence information from many sources, from the intelligence community (IC) and law enforcement and from IAIP, which as a member of the IC, routinely receives information from intelligence and law enforcement partners. IAIP has the overall responsibility at DHS for receipt and analysis of information related to threats to the homeland. TSA activated the Transportation Security Operations Center (TSOC) in 2003 to serve as a single point of contact for security-related operations, incidents, or crises in aviation and all land modes of transportation. The National Capital Region Command Center is co-located with the TSOC and provides seamless integration in protecting the National Capital Region. TSA's 24-hour watch routinely communicates with industry representatives about security events or information of potential security interest.

TSA also has electronic connectivity to intelligence community databases and participates in daily intelligence teleconferences with other Federal agencies to discuss threat and incident reports. To ensure that all information pertinent to transportation security is identified and provided to TSA on a timely basis, TSA has assigned liaison

officers to major intelligence and law enforcement agencies. TSA also receives reporting through its field personnel on security incidents that occur at airports and aboard aircraft and from local law enforcement. This information is transmitted to TSA headquarters for evaluation and appropriate dissemination to intelligence and law enforcement agencies. TSA coordinates with IAIP to disseminate specific warnings, advisory information, or countermeasures, where appropriate, to local law enforcement and the transportation industry. All threat information received by the TSA, including information not specifically mentioning transportation, is carefully reviewed for its potential impact on any U.S. transportation asset at home or overseas. TSA consults with other security and technical experts within DHS and in other agencies to achieve a comprehensive threat and vulnerability assessment. If we conclude that warnings to industry and field operators or operational adjustments are warranted, our response can take a variety of forms. Top government decision makers are alerted immediately, as well as industry stakeholders.

The next step in our threat-based, risk-managed approach is to assess the criticality of the Nation's transportation infrastructure assets. Leveraging processes developed by IAIP, TSA developed a criticality model and is now deploying this model to determine criticality scores for facilities and assets. The vulnerability assessment process examines the overall security posture of a transportation asset as well as the security posture of the asset in response to identified threat scenarios. TSA has developed vulnerability assessment tools in concert with DOT modal administrations and industry stakeholders. For assets determined to be critical, the Transportation Risk Assessment and Vulnerability Tool (TRAVEL) will assess an asset's baseline security system and that system's effectiveness in detecting, deterring, and/or preventing potential threats. For assets determined to be less critical, TSA recommends the use of self-assessment tools. To date, one self-assessment module has been developed, in conjunction with CG, for use in the maritime transportation mode. Additional modules will be created for the other transportation modes. For the aviation mode, a third tool, the Joint Vulnerability Assessment (JVA) will also be utilized in conjunction with the FBI at critical commercial airports. Using the results of the vulnerability assessments, we can collectively develop targeted, layered security measures tied to DHS threat levels, or specific intelligence, with maximum flexibility to allow for normal transportation activity even during periods of elevated threat.

Securing Surface Transportation

DHS, in close coordination with our partners at DOT, state and local governments, and transit and rail operators, has taken a number of steps to address vulnerabilities in the rail and transit systems and improve our security posture against attacks. These efforts span the spectrum of security, from information sharing and awareness through prevention, response and recovery to a potential terrorist attack in the United States.

The Department, working with the Federal Transit Administration (FTA), coordinates information and threat sharing for rail and transit through the FTA-funded Surface Transportation Information Sharing and Analysis Center (ST-ISAC) in partnership with

the Association of American Railroads (AAR) and the American Public Transportation Association. As part of the significant partnership that has developed, TSA hosts ST-ISAC representatives at the TSOC. When appropriate, DHS disseminates Information Bulletins describing specific threats and providing suggested protective measures. In addition, DHS hosts conference calls with our Federal, state, local, and industry partners to communicate current information, obtain an assessment of the level of related preparedness, and determine additional short-term measures to be taken. For example, in the immediate aftermath of the Madrid attacks, the Department released two Information Bulletins and hosted National Conference Calls with federal, state and local public safety communities, all State and Territorial Homeland Security Advisors, officials from 50 major urban areas, and industry stakeholders.

Prior to the Madrid and Moscow events, criticality assessments of rail and transit networks operating in high-density urban areas were performed by TSA and FTA, and as a result of these assessments, these systems have produced robust security and emergency preparedness plans. Between FY 2003 and this year, DHS has used information from these assessments to allocate \$115 million to high-risk transit systems through the Urban Area Security Initiative (UASI) in the Office for Domestic Preparedness. Sixty-five million dollars (\$65 million) was allocated in fiscal year 2003 and \$50 million was allocated in fiscal year 2004. Grantees may use these funds for such expenses as the installation of physical barricades, video surveillance systems, motion detectors, thermal/IR imagery and chemical/radiological material detection systems, integrated communications systems, and for prevention planning, training and exercises, among other things.

TSA has partnered with the FTA on its "Transit Watch" Program, and is coordinating with the Federal Railroad Administration (FRA) to develop a rail system inspection guide for use by rail law enforcement and security personnel to inspect trains for explosives and other threats. The Department's Federal Law Enforcement Training Center has provided security training to rail and transit operators, and TSA has distributed educational information to transit system employees on how to recognize and respond to potential terrorist attacks.

TSA has also hosted security exercises to bring together rail carriers, federal and local first responders, and security experts, to address potential gaps in antiterrorism training among rail personnel. One such security exercise occurred at Union Station in Washington, DC, in July 2003, and involved stakeholders, emergency responders and enforcement agencies all working to implement the station's Emergency Response Plan. In another security exercise, DHS, through TSA, partnered with the Naval War College Gaming Department to conduct an operation designed to evaluate security awareness, prevention, response and recovery of the national transportation system to a security incident. The lessons learned from these exercises are being used to enhance rail security for the entire Northeast corridor.

The mass transit and rail industries, and State and local governments, have been very proactive in addressing homeland security issues. Most recently, transit and rail system

operators enhanced their existing security plans by taking additional preventive measures in cooperation with the Department, including more canine and uniformed patrols, increased surveillance, and reporting and awareness campaigns in the passenger environment. Rail cargo companies are continuing their Alert Level 2, which includes increased security at designated facilities, security plan review, and increased spot identification checks.

On March 22, Secretary of Homeland Security Tom Ridge announced additional measures to strengthen our rail and transit systems. Building on many of the security measures recommended for mass transit and passenger rail authorities, the Department is engaging our Federal partners at DOT, the industry, and state and local authorities to establish base-line security measures based on current industry best practices. These include existing security measures currently being implemented consistently in the mass transit systems and the commuter rail environment and could be adjusted in consultation with transit and rail system owners and operators in response to higher threat levels or specific threats in the future. DHS will ensure compliance with security standards for commuter and rail lines.

TSA is implementing a pilot program in New Carrollton, Maryland, to test the feasibility of using emerging technologies for screening passengers and carry-on items for explosives at rail stations and aboard trains. This pilot, the Transit and Rail Inspection Pilot (TRIP), is being conducted in partnership with AMTRAK, MARC, WMATA, and DOT for a 30-day period. Additional phases of the pilot program are under consideration. The pilot program does not resemble an aviation-type solution to transit and rail security challenges, but rather provides a venue to test new technologies and screening concepts. Rail stations are not self-contained, and passengers have the freedom to board and disembark trains throughout their routes. The lessons learned from the pilot could allow transit operators to deploy targeted screening in high threat areas or in response to specific intelligence.

Using existing Homeland Security explosive detecting canine resources, the Department is developing a rapid deployment Mass Transit canine program. These mobile response teams will be prepared to assist local law enforcement teams. The Federal Protective Service will lead an effort to ensure canine teams from various DHS agencies are cross-trained for the rail and transit environment and available for augmentation of local capabilities when needed. DHS will partner with local authorities to provide additional training and assistance for local canine teams. The mobile program would be used predominantly in special threat environments and provide additional federal resources to augment state and local transit and rail authorities' security measures.

The Department also plans to leverage existing efforts to generate additional public awareness by integrating existing passenger and rail education materials and awareness programs developed by industry, TSA, and FTA. The Department's Federal Law Enforcement Training Center will also accelerate current security training programs for transit law enforcement personnel.

DHS's Advanced Research Project Agency is developing a program that will focus on research and development of next generation technology for High Explosives Countermeasures. The goal of the program is to develop and test field equipment, technologies and procedures to interdict suicide bombers and car and truck bombs before they can reach their intended targets while minimizing the impact on the freedom of movement. Research and development efforts such as this will be closely coordinated with TSA to ensure that research and development activities lead to deployable solutions.

For highway security, TSA entered into a \$19.3 million cooperative agreement with the American Trucking Associations (ATA) to expand the Highway Watch program. The program trains highway professionals to identify and report safety and security situations on our Nation's roads. The expanded program will provide training and communications infrastructure to prepare 400,000 transportation professionals to respond in the event they or their cargo are the target of a terrorist attack and to share valuable intelligence with TSA if they witness potential threats.

Under the USA PATRIOT Act, TSA is also required to conduct security threat assessments on drivers holding a hazardous materials (HAZMAT) endorsement on a commercial driver's license. This effort is being pursued in two phases: name-based, terrorist-focused checks will be conducted on all 3.5 million HAZMAT drivers by June 2004; and fingerprint-based criminal history records checks will begin by January 31, 2005. TSA is working closely with the States and the private sector to develop the necessary infrastructure to establish this program. TSA also plans to leverage existing capabilities and infrastructure when possible to institute the security threat assessment.

DHS has a substantial effort under way to strengthen security credential programs across the Department. For our part, TSA is testing alternatives for a Transportation Worker Identification Credential (TWIC) to mitigate potential threats posed by workers and those with fraudulent identification. During the current prototype stage, beginning this summer, this credential will test the feasibility of bringing uniformity and consistency to the process of granting access to transportation workers entrusted to work in the most sensitive and secure areas of our national transportation system.

With our Federal government's security capabilities now under one roof, in one department, the level of communication and cooperation in enhancing intermodal cargo supply chain security among the CG and BTS agencies, including ICE, CBP, and TSA, is stronger than ever. BTS is leading the effort, with TSA, CBP, and the CG, to develop a more comprehensive framework for securing the intermodal cargo supply chain. This initiative will also assist in meeting Maritime Transportation Security Act requirements for Secure Systems of Transportation by incorporating a point of origin to point of destination approach to cargo transportation. Agencies are reviewing cargo program, analytic tools, and other relevant resources within the Department to identify remaining supply chain vulnerabilities.

TSA is providing CG with technical assistance in the development of methods for local operator inspection of passengers and vehicles using established ferry transportation

systems. TSA is implementing the “Synergy Project” designed to test the long-term feasibility of screening and transferring passenger baggage from seaport to airport, reducing the congestion at airport security checkpoints caused by the influx of large number of passengers disembarking from cruise ships. This program is currently underway at the ports of Miami and Vancouver.

Securing the Civil Aviation System

When it was created, TSA inherited a 30-year-old aviation security system. With the help of its many partners, TSA has created a new system that is dramatically different from that which was in place on September 11, 2001. TSA’s fundamental strategy in operating this system includes establishing a system of rings of security whereby each security ring contributes to our overall aviation security system, but we do not rely exclusively on any one component.

As in other transportation modes, we begin aviation security with domain awareness. TSA continuously gathers as much information as possible about the threats, vulnerabilities, trends, and conditions of the aviation system and its environment. This first ring in our system-of-systems enables TSA to prioritize, direct resources, and take protective action.

TSA and the Federal Aviation Administration (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. TSA has required background checks to be performed on more than a million air carrier and airport employees with unescorted access to airport secured and sterile areas. Across the country 158 Federal Security Directors (FSDs) lead and coordinate all TSA security activities at airports, including tactical planning, execution, and operating management. At checkpoints, highly trained, qualified personnel screen passengers and carry-on items using state-of-the-art metal detectors. All checked baggage is screened using a combination of explosives detection systems (EDS), explosives trace detection machines (ETD), and where necessary, other congressionally approved methods of screening.

Each day, TSA intercepts more than 15,000 prohibited items at airports around the country. Each month more than 40 firearms are intercepted at airport checkpoints by TSA screeners. This tells us first, that we must continue to be diligent in our screening efforts, and second, that many passengers are not voluntarily complying with the ban on bringing prohibited items onto aircraft. While the majority of cases are not intentional violations, too frequently individuals are deliberately attempting to circumvent security or test the security system. We have intercepted a knife concealed inside a soda can, a sword hidden inside a cane, and a knife hidden within a prosthetic leg, just to name a few examples. TSA has held press conferences at many airports around the country to educate passengers about prohibited items. We prominently post signs in airports to help passengers understand which items are prohibited, and we provide detailed information on our public website.

TSA uses its Special Operations Program to provide ongoing and immediate feedback to screeners, their supervisors, and TSA leadership on screener performance. The Special Operations Program's overall objectives are to test the security systems at the airports and to introduce difficult, real-life threat items to the screener workforce. Once covert testing is completed at a checkpoint, Special Operations teams conduct post-test reviews with available screeners to reenact the test and provide training. These tests are based on the latest intelligence and are far more rigorous than any security testing conducted prior to 9/11. Despite continually raising the bar on these tests, TSA's screeners and security systems continue to improve over time. However, the primary goal of these tests is not to show improvement. We make our system testing hard, harder, and harder still, to uncover vulnerabilities and to address them.

To maintain high levels of screener proficiency, TSA's Screening Improvement Plan places a strong emphasis on recurrent screener training and supervisory training. Over 700 inert Modular Bomb Set (MBS II) and weapons training kits have been deployed to every airport in the country as an integral part of TSA's recurrent training for screeners, enabling them to see and touch the components of improvised explosive devices and weapons. TSA is also developing protocols to help FSDs conduct their own airport level screening testing. To blend nationally and locally developed training, TSA has established the "Excellence in Screener Performance" video training series. The third part of our recurrent training program is a series of web-based and computer-based screener training programs. Recognizing the need to provide our front line supervisors with the tools they need to manage the screener workforce effectively, TSA has sent more than 3500 supervisors to introductory leadership training at the Graduate School, United States Department of Agriculture.

TSA's Threat Image Projection (TIP) program is an essential element of TSA's screening improvement plan. All checkpoint security lanes now are equipped with TRXs with the 2400-image TIP library, providing real-time data on screener performance. Data is available quickly at the local level and reported to headquarters for aggregated analysis and monitoring. Through deployment of TRX machines and activation of the expanded TIP image library, TSA is able to collect and analyze significant amounts of performance data that has not been previously available. TIP is an excellent tool for evaluating the skills of each individual screener so that we can focus directly on areas needing skill improvement. By regularly exposing screeners to a variety of threat object images, TIP provides continuous on-the-job training and immediate feedback.

Today TSA is right-sizing and stabilizing screening operations based on security requirements and opportunities for increasing efficiencies in business processes. As part of our workforce planning, we are evolving to a business model that vests more hiring authority at the local level with our FSDs to address airport staffing needs. The original methods we used in centralizing recruitment, assessment, hiring, and training of screeners were necessary in the fast-paced environment to meet the original statutory deadlines. However, this highly centralized model is not the right fit for sustaining an existing workforce.

Although the Aviation and Transportation Security Act mandated the federalization of airport security screening, it held open the possibility that airports could return to contract screening, provided the high standards required by law and instituted by TSA are met. TSA is currently operating a pilot program at five airports using private screeners that, by law, must meet TSA eligibility, training, and performance requirements and receive pay and other benefits not less than 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. A recent evaluation by BearingPoint will assist us in assessing if and how to expand contract screening. The report found that the private screening pilot airports performed at essentially the same level as federally screened airports. Overall, we believe the report confirms that TSA has been successful in ensuring equal security at the five participating airports. We look forward to applying the insights detailed within the report and the lessons learned from the pilot program as we consider guidance and procedures for airports to opt out of Federal screening.

EDS/ETD equipment purchase and installation is the key to compliance with statutory requirements for full electronic screening of checked baggage. TSA purchases and installs this equipment through a variety of mechanisms, including congressionally authorized Letters of Intent (LOIs), which provide a partial reimbursement to airports for facility modifications required to install in-line EDS solutions. TSA has issued eight airport LOIs, covering nine airports. TSA is also using resources to purchase and install EDS and ETD machines at airports outside the LOI process.

Our National Explosives Detection Canine Team program performs a critical role in aviation security, performing multiple tasks throughout the entire airport environment, such as screening checked baggage, searching unattended bags, searching vehicles approaching terminals during increased threat levels, screening cargo on a limited basis, screening mail at certain pilot project locations, and responding to bomb threats. TSA helps local law enforcement agencies by procuring and training selected canines, training selected law enforcement officers, and by partially reimbursing agencies for costs.

The number of Federal Air Marshals (FAMs) was increased from just a few on 9/11 to thousands today, and they are now deployed on high-risk domestic and international flights. With the transfer of the FAM Service from TSA to ICE, BTS has the flexibility to deploy additional ICE agents as a surge force to temporarily increase the number of FAMs on high-risk flights when threat conditions warrant.

In light of security concerns, TSA is performing security checks on flight crew on domestic and international passenger and cargo flights bound for the U.S. TSA will also assume responsibility this summer for conducting background checks on aliens who wish to undergo flight training in the United States. Vision 100 transferred this requirement from the Department of Justice to TSA.

In addition, commercial aircraft serving the U.S. are equipped with new, hardened cockpit doors. TSA, working with its U.S. government partners through the International

Civil Aviation Organization (ICAO), is seeking to encourage compliance of foreign carriers with the international requirement for hardened cockpit doors, which went into effect November 2003.

Training of pilots who volunteer for TSA's Federal Flight Deck Officer (FFDO) program will continue at a strong pace with requested funding of \$25 million in FY 2005. On May 1, the first prototype FFDO class of cargo pilots graduated. TSA initiated the on-line application process for cargo and other flight deck crew members in February 2004. In January 2004, TSA began doubling the number of FFDO classes, and we plan to provide initial training and qualification for thousands of FFDOs by the end of this fiscal year. TSA has streamlined the process for pilots to become FFDOs, and candidate assessments are administered at 52 locations throughout the United States, with more being added. Pilots also must attend re-qualification sessions twice a year to ensure that they maintain a high level of proficiency and familiarity with program requirements. Ten private, state, and local government sites are available for self-scheduling of re-qualification training. As the number of FFDOs grows, TSA will consider expanding the number of recurrent training sites to meet their needs.

Ensuring that flight and cabin crew members receive self-defense training will add another layer of security for in-flight aircraft. Each of these security enhancements is an additional obstacle that a terrorist would have to overcome in order to accomplish his objective. Each has been carefully developed with attention to security, customer service, and a minimum impact on the flow of commerce.

TSA plans to institute a Registered Traveler (RT) Pilot Program in the summer of 2004 at a limited number of airports. RT pilots will last approximately 90 days. TSA anticipates that an RT program could provide both security and customer service benefits. TSA envisions that an RT Program would be voluntary and may offer those qualified an expedited travel experience as they go through the screening checkpoint. A security assessment will be conducted on each RT applicant to determine eligibility for the program. Upon conclusion of the Pilots, results will be analyzed to determine the best program approach for proceeding on a larger scale program.

A total of \$60 million is requested for FY 2005 for the second generation Computer Assisted Passenger Pre-screening System (CAPPS II). CAPPS II is a limited, automated prescreening system authorized by Congress. Developed with the utmost concern for individual privacy rights, CAPPS II would modernize the prescreening system currently implemented by the airlines. CAPPS II is expected to employ technology and data analysis techniques to conduct an information-based identity authentication for each passenger using commercial information along with data each passenger provides to the airline upon making a reservation. CAPPS II will combine the results (scores) from the identity authentication with a risk assessment. The overall process will yield a recommended screening level, based on the degree of risk assessed, or specific identifiable terrorist threat. The commercially available data will not be viewed by government employees, and intelligence information will remain behind the government

firewall. The entire prescreening process is expected to take only a few seconds to complete.

In its recent report on CAPPs II, the GAO concluded that in most areas that Congress asked them to review, our work on CAPPs II is not yet complete. DHS has generally concurred in GAO's findings, which in our view validates the fact that CAPPs II is a program still under development. As we resolve issues of access to data needed for testing CAPPs II, and the testing phase moves forward and results in a more mature system, we are confident of our ability to satisfy all of the questions that Congress posed.

Each year, U.S. air carriers transport approximately 12.5 million tons of cargo. To deny terrorists the opportunity to exploit our thriving air cargo system, TSA has developed an Air Cargo Strategic Plan that calls for the focused deployment of tools, resources, and infrastructure that are available today, as well as creating a foundation for future improvements as technology and resources become available. TSA has prohibited all "unknown shipper" cargo from flying aboard passenger carriers since September 11, 2001, thereby limiting cargo to packages from identifiable shippers under the TSA Known Shipper program. TSA has enhanced the criteria for participation in the Known Shipper program and is rolling out an automated Known Shipper database that will allow air carriers and indirect air carriers to verify immediately the status of a specific shipper. TSA has also mandated inspections of a certain amount of cargo transported aboard both passenger and all cargo aircraft.

Under the Air Cargo Strategic Plan, TSA will work closely with CBP to establish a Cargo Pre-Screening system that identifies which cargo should be considered "high-risk" and work with industry and other federal agencies and the airline and shipping industries to ensure that 100 percent of high-risk cargo is inspected. We are also partnering with stakeholders to implement enhanced background checks on persons with access to cargo and new procedures for securing aircraft while they are on the ground. TSA and CBP are working together on air cargo initiatives through four established work groups, making plans for future collaboration, leveraging of existing programs, and sharing resources and technologies.

TSA is requesting \$55 million in FY 2005 for the continuation of an aggressive R&D program to investigate technologies that will improve our ability to screen high-risk cargo. TSA will look at new technologies for screening large cargo, including pallets and containerized cargo. In January 2004, TSA issued a market survey requesting submissions and participation of vendors of commercial off-the-shelf explosives detection technology to support cargo inspection. A number of vendors have been tentatively selected for laboratory evaluation of their products against the current EDS certification criteria. TSA has issued a request for proposals (RFP) for potential inventors of explosives detection technology for the screening of containerized cargo and U.S. mail to be transported on passenger aircraft. This RFP, which resulted in 74 responses, will lead to the award of R&D grants to assist in the development of promising technologies. At TSA's state-of-the-art research laboratory, the Transportation Security Laboratory (TSL), we are conducting a cargo characterization study to determine the

feasibility of using currently deployed explosives detection technology (EDS and ETD) to screen cargo while new systems are under development.

We need to stay at least one step ahead at all times in the development of new security technology. The President's FY 2005 Budget request includes \$49 million for applied research and development and \$50 million for next-generation EDS. TSA has a robust research and development program and works closely with DHS S&T to develop and deploy technology that will help make operations more effective, more efficient, less time consuming, and less costly. I would like to invite the Subcommittee to visit our TSL to see the full scope of efforts underway. Several screening and other security technologies are under development, including an explosives detection portal for passengers to determine if explosives are being carried on an individual's person, document scanners to detect trace amounts of explosive materials on items such as boarding passes, and scanners for better screening of casts and prosthetic devices.

DHS, in partnership with other federal agencies, is taking an aggressive approach to counter the threat of Man Portable Air Defense Systems (MANPADS) to civilian commercial aircraft. The strategy includes proliferation control, tactical measures and recovery, and technical countermeasures. In January, DHS S&T announced the selection of teams to develop plans and test prototypes to help determine whether a viable technology exists that could be deployed to address the potential threat of MANPADS. In addition, as part of the overall MANPADS strategy, TSA is performing airport vulnerability assessments to identify and map the areas around an airport from which a MANPADS attack could be initiated and working with surrounding communities to coordinate the efforts of agencies responsible for responding to this type of threat.

I appreciate this opportunity to highlight just a portion of TSA's efforts and progress in improving transportation security. There is no doubt that securing our nation's transportation system will be both costly and time consuming. Distributing these costs fairly and equitably is a constant challenge—and a constant goal. Looking ahead to Fiscal Year (FY) 2005, TSA and our many partners at the Federal, state, and local levels, and in the private sector, will continue to reinforce transportation security through innovation, technology and enhanced performance. In the two years since its creation, TSA has developed a culture of immediacy and a strong commitment to continual improvement. The increased variety and sophistication of weapons and communication tools available to modern terrorists presents a significant challenge. With preventive measures in place, the risk of terrorism is reduced, albeit not eliminated. TSA will continue to identify and re-evaluate threats and vulnerabilities and make decisions that both facilitate transportation and improve its security.

I will be pleased to answer your questions.