KNIVES, BOX CUTTERS, AND BLEACH: A REVIEW OF PASSENGER SCREENER TRAINING, TESTING AND SUPERVISION

HEARING

BEFORE THE

COMMITTEE ON GOVERNMENT REFORM

HOUSE OF REPRESENTATIVES

ONE HUNDRED EIGHTH CONGRESS

FIRST SESSION

NOVEMBER 20, 2003

Serial No. 108–117

Printed for the use of the Committee on Government Reform

Available via the World Wide Web: http://www.gpo.gov/congress/house
http://www.house.gov/reform

U.S. GOVERNMENT PRINTING OFFICE

92–440 PDF WASHINGTON : 2004

For sale by the Superintendent of Documents, U.S. Government Printing Office
Internet: bookstore.gpo.gov Phone: toll free (866) 512–1800; DC area (202) 512–1800
Fax: (202) 512–2250 Mail: Stop SSOP, Washington, DC 20402–0001

COMMITTEE ON GOVERNMENT REFORM

TOM DAVIS, Virginia, *Chairman*

DAN BURTON, Indiana
CHRISTOPHER SHAYS, Connecticut
ILEANA ROS-LEHTINEN, Florida
JOHN M. MCHUGH, New York
JOHN L. MICA, Florida
MARK E. SOUDER, Indiana
STEVEN C. LATOURETTE, Ohio
DOUG OSE, California
RON LEWIS, Kentucky
JO ANN DAVIS, Virginia
TODD RUSSELL PLATTS, Pennsylvania
CHRIS CANNON, Utah
ADAM H. PUTNAM, Florida
EDWARD L. SCHROCK, Virginia
JOHN J. DUNCAN, JR., Tennessee
JOHN SULLIVAN, Oklahoma
NATHAN DEAL, Georgia
CANDICE S. MILLER, Michigan
TIM MURPHY, Pennsylvania
MICHAEL R. TURNER, Ohio
JOHN R. CARTER, Texas
WILLIAM J. JANKLOW, South Dakota
MARSHA BLACKBURN, Tennessee

HENRY A. WAXMAN, California
TOM LANTOS, California
MAJOR R. OWENS, New York
EDOLPHUS TOWNS, New York
PAUL E. KANJORSKI, Pennsylvania
CAROLYN B. MALONEY, New York
ELIJAH E. CUMMINGS, Maryland
DENNIS J. KUCINICH, Ohio
DANNY K. DAVIS, Illinois
JOHN F. TIERNEY, Massachusetts
WM. LACY CLAY, Missouri
DIANE E. WATSON, California
STEPHEN F. LYNCH, Massachusetts
CHRIS VAN HOLLEN, Maryland
LINDA T. SANCHEZ, California
C.A. "DUTCH" RUPPERSBERGER, Maryland
ELEANOR HOLMES NORTON, District of Columbia
JIM COOPER, Tennessee
CHRIS BELL, Texas

BERNARD SANDERS, Vermont (Independent)

PETER SIRH, *Staff Director*
MELISSA WOJCIAK, *Deputy Staff Director*
ROB BORDEN, *Parliamentarian*
TERESA AUSTIN, *Chief Clerk*
PHILIP M. SCHILIRO, *Minority Staff Director*

CONTENTS

	Page
Hearing held on November 20, 2003	1
Statement of:	
Berrick, Cathleen A., Director, Homeland Security and Justice Issues, General Accounting Office; John DeMell, president, Firstline Transportation Security; and James McNeil, chief executive officer, McNeil Technologies, Inc., accompanied by Mike Broida, site manager, Greater Rochester International Airport	48
McHale, Stephen, Deputy Administrator, Transportation Security Administration	17
Letters, statements, etc., submitted for the record by:	
Berrick, Cathleen A., Director, Homeland Security and Justice Issues, General Accounting Office, prepared statement of	51
Burton, Hon. Dan, a Representative in Congress from the State of Indiana, prepared statement of	112
Cummings, Hon. Elijah E., a Representative in Congress from the State of Maryland, prepared statement of	117
Davis, Chairman Tom, a Representative in Congress from the State of Virginia, prepared statement of	5
DeMell, John, president, Firstline Transportation Security, prepared statement of	85
McHale, Stephen, Deputy Administrator, Transportation Security Administration, prepared statement of	21
McNeil, James, chief executive officer, McNeil Technologies, Inc., prepared statement of	96
Ruppersberger, Hon. C.A. Dutch, a Representative in Congress from the State of Maryland, prepared statement of	12
Waxman, Hon. Henry A., a Representative in Congress from the State of California, prepared statement of	114

KNIVES, BOX CUTTERS, AND BLEACH: A REVIEW OF PASSENGER SCREENER TRAINING, TESTING AND SUPERVISION

THURSDAY, NOVEMBER 20, 2003

HOUSE OF REPRESENTATIVES,
COMMITTEE ON GOVERNMENT REFORM,
Washington, DC.

The committee met, pursuant to notice, at 10:45 a.m., in room 2154, Rayburn House Office Building, Hon. Tom Davis (chairman of the committee) presiding.

Present: Representatives Tom Davis of Virginia, Shays, Mica, Souder, Platts, Murphy, Carter, Janklow, Blackburn, Kanjorski, Tierney, Watson, Van Hollen, Sanchez, Ruppersberger and Norton.

Staff present: Melissa Wojciak, deputy staff director; Jennifer Safavian, chief counsel for oversight and investigations; Anne Marie Turner and David Young, counsels; David Marin, director of communications; John Cuaderes, senior professional staff member; Teresa Austin, chief clerk; Brien Beattie, deputy clerk; Allyson Blandford, office manager; Corinne Zaccagnini, chief information officer; Michael Yeager, minority deputy chief counsel; David Rapallo, minority counsel; Earley Green, minority chief clerk; and Jean Gosa, minority assistant clerk.

Chairman TOM DAVIS. Good morning. A quorum being present, the committee will come to order.

We are here today to examine a key aspect of airport security: passenger screeners. This is the committee's first hearing into airport security issues, but it is a good bet it will not be the last.

There is no alternative but success in securing our Nation's air system. As such, it is critical that Congress, and this committee in particular, be vigilant in our oversight obligations. That is why last month this committee started an extensive review of the Transportation Security Administration's operations, with a specific focus on passenger and baggage screeners. This review was prompted by the discovery of weapons and other prohibited items on two Southwest Airline planes on October 16th, as well as the recent reports from the Department of Homeland Security's Office of Inspector General and the General Accounting Office that cited significant weaknesses in the testing and training procedures for TSA airport screeners.

Approximately 1.8 million travelers a day pass through checkpoints at more than 400 U.S. airports. The daunting task of protecting America's transportation system could not be more critical in today's threat environment. The good news is that in just 2

years, TSA has made tremendous progress promoting security by hiring and training 48,000 Federal passenger screeners. The screeners are better paid and better trained, and we are safer today because of it. I don't think we should lose sight of that.

TSA passenger screeners have seized significant numbers of prohibited items from passengers going through security checkpoints. But despite this fact and the realization that not all prohibited items will be detected at passenger checkpoints, these recent security breaches have highlighted possible weaknesses in the system that need to be addressed.

In six separate incidents, beginning February 7, 2003, and ending September 14, 2003, Mr. Nat Heatwole, a 20-year-old college student, was allegedly able to get prohibited items, including box cutter blades, knives, and liquid bleach, past airport passenger screeners and onto aircraft. Notes accompanying the items he allegedly left on the aircraft indicated that the items were intended to test the TSA checkpoint security procedures. On September 15, 2003, TSA's Contact Center also received an e-mail message from Mr. Heatwole concerning the security breaches. However, the message was not delivered to appropriate TSA officials until October 17, 2003, after some of the prohibited items had been accidentally found, and after TSA ordered 7,000 aircraft to be searched.

The delay in identifying Mr. Heatwole's September 15 e-mail as an important message that required immediate action highlighted problems with TSA's Contact Center. The committee understands that TSA has identified the problems within the Contact Center and has modified procedures by which messages are handled at the Center. This last Friday I went on a tour of the Transportation Security Coordination Center, out in northern Virginia, which utilizes information from the Contact Center, the Federal air marshals and other sources to take action in cases of aviation security concerns. From what I saw, the Coordination Center stands ready 24 hours a day, 7 days a week to act on aviation emergencies, but it must receive timely information to take action. We look forward to hearing the steps TSA has taken to remedy the problem to ensure that future security-related messages like Mr. Heatwole's are immediately analyzed by TSA staff and that appropriate action is taken.

I understand that Mr. Heatwole has cooperated fully with the TSA and FBI, and he has been forthcoming with this committee in sharing his intentions behind these security breaches. The public opinion of Mr. Heatwole's actions seem to range from "hero" to "criminal." It is up to the justice system to determine the consequences of his actions. I personally believe we need to discourage this sort of vigilante behavior. It is counterproductive for TSA, law enforcement and the airlines to waste valuable time and resources on similar incidents when we need them to be looking for real threats. Again, we have internal tests going on every day from the IG, GAO, and other offices finding this. The results are being relayed to TSA. But I do think we should acknowledge that Mr. Heatwole's actions have provided us a chance to have a thoughtful discussion on improving passenger screening. Experience, no matter its cause or origin, is the best teacher.

In addition to hearing about TSA's reaction to the Nat Heatwole incident today, we also have the opportunity to discuss recent gov-

ernment work to review TSA training, testing and supervision of passenger screeners. The investigation by DHS IG found that TSA written tests for potential passenger screeners on the operation of explosive detention system machines were designed to maximize the likelihood TSA employees would pass, rather than ensuring that only competent and well-trained employees were responsible for passenger screening. In essence, they have been teaching to the test. More disconcerting was the DHS IG's covert testing of passenger security screening operations. According to press articles, IG investigators were able to bring knives, a bomb and a gun through Boston's Logan International Airport without being detected.

The GAO report cited deficient supervisory training programs and a failure to collect adequate information on screener performance in detecting threat objects. The report also cited the need for recurrent training for passenger screening, to ensure that screener skills are maintained and enhanced as new security information becomes available. In addition, the GAO report found that Federal Security Directors, who are responsible for overseeing security at the airports, have expressed concern that they have limited authority to respond to airport-specific staffing needs. These needs include daily and seasonal fluctuations in passenger flow. We look forward to hearing more from GAO about their report during our second panel of witnesses.

TSA has stated that new procedures for passenger screener training and testing are in the works, including new written tests to replace the tests criticized in the DHS IG report. In addition, specific training courses designed for screener supervisors are being developed to improve screener performance. We are anxious to hear about these new changes.

There are currently five pilot program airports that use private companies to provide passenger screener functions. These private companies were responsible for developing and implementing training for passenger screeners prior to the Federalization of passenger screeners by TSA and therefore have significant experience in the business of training, testing and supervision. We are pleased to have representatives from two of the private pilot program airports, the Kansas City International Airport in Missouri and the Greater Rochester International Airport in New York, on our second panel. We look forward to their testimony and hope to hear about their relationship with TSA, suggestions for improvements with the new Federal work force, and how the pilot program has worked with regard to passenger screener training, testing and supervision.

The committee is mindful that the holiday season has begun and that the traveling rush will inevitably result in longer lines at checkpoints. TSA has the immense task of maintaining adequate staffing levels for passenger screening over the next month and a half. At the same time, TSA passenger screeners will face additional pressure to process passengers quickly, despite the fact that they are not permitted to allow passengers into airport sterilized areas without resolving all possible threats identified in both passenger and carry-on baggage checks. But security measures at airports cannot be compromised. As travelers, we need to be prepared for rigorous security checks, and I hope that TSA can give us some

advice today about how travelers can smoothly proceed through passenger screening checkpoints.

We look forward to a constructive hearing today, keeping in mind that no system is foolproof. In fact, keeping prohibited items off a passenger plane is but one layer of a multi-layered aviation security strategy, which includes hardened cockpit doors, additional Federal air marshals, and armed pilots. The airlines have taken their own steps to increase the number of layers, by training their flight attendants in self-defense, for example. However, a chain is only as strong as its weakest link, and we are hopeful that our oversight of TSA passenger screener training, testing and supervision will improve overall aviation security.

[The prepared statement of Chairman Tom Davis follows:]

Statement of Chairman Tom Davis
Government Reform Committee Hearing
"Knives, Box Cutters, and Bleach: A Review of Passenger Screener Training, Testing and Supervision"
November 20, 2003

We are here today to examine a key aspect of airport security: passenger screeners. This is the Committee's first hearing into airport security issues, but it's a good bet it will not be the last. There is no alternative but success in securing our nation's air system. As such, it is critical that Congress, and this Committee in particular, be vigilant in our oversight obligations. That is why last month, this Committee started an extensive review of the Transportation Security Administration's operations, with a specific focus on passenger and baggage screeners. This review was prompted by the discovery of weapons and other prohibited items on two Southwest Airline planes on October 16th; as well as the recent reports from the Department of Homeland Security Office of Inspector General Report and the General Accounting Office that cited significant weaknesses in the testing and training procedures for TSA airport screeners.

Approximately 1.8 million travelers a day pass through checkpoints at more than 400 U.S. airports. The daunting task of protecting America's transportation system could not be more critical in today's threat environment. The good news is that in just two years, TSA has made tremendous progress promoting security by hiring and training 48,000 federal passenger screeners. The screeners are better paid and better trained, and we are safer today because of it. TSA passenger screeners have seized significant numbers of prohibited items from passengers going through

security checkpoints. But despite this fact and the realization that not all prohibited items will be detected at passenger checkpoints, these recent security breaches have highlighted possible weaknesses in the system that need to be addressed.

In six separate incidents, beginning February 7, 2003 and ending September 14, 2003, Mr. Nat Heatwole, a twenty-year-old college student, was allegedly able to get prohibited items, including box cutter blades, knives, and liquid bleach, past airport passenger screeners and onto aircraft. Notes accompanying the items he allegedly left on the aircraft indicated that the items were intended to test the TSA checkpoint security procedures. On September 15, 2003, TSA's Contact Center also received an e-mail message from Mr. Heatwole concerning the security breaches; however, the message was not delivered to appropriate TSA officials until October, 17, 2003, **AFTER** some of the prohibited items had been accidentally found and **AFTER** TSA ordered 7,000 aircraft to be searched.

The delay in identifying Mr. Heatwole's September 15th e-mail as an important message that required immediate action highlighted problems with TSA's Contact Center. The Committee understands that TSA has identified the problems within the Contact Center and has modified procedures by which messages are handled at the Center. This last Friday, I went on a tour of the Transportation Security Coordination Center, which utilizes information from the Contact Center, the Federal Air Marshals, and other sources to take action in cases of aviation security concerns. From what I saw, the Coordination Center stands ready twenty-fours a day, seven days a week, to act on aviation emergencies, but it must receive timely information

to take action. We look forward to hearing the steps TSA has taken to remedy the problem to ensure that future security-related messages, like Mr. Heatwole's, are immediately analyzed by TSA staff and that appropriate action is taken.

I understand that Mr. Heatwole has cooperated fully with the TSA, and FBI, and he has been forthcoming with this Committee in sharing his intentions behind these security breaches. The public opinion of Mr. Heatwole's actions seems to range from "hero" to "criminal." It is up to the justice system to determine the consequences of his actions. I personally believe we need to discourage this sort of vigilante behavior. It is counterproductive for TSA, law enforcement, and the airlines to waste valuable time and resources on similar incidents when we need them to be looking for real threats. But I do think, we should acknowledge that Mr. Heatwole's actions have provided us a chance to have a thoughtful discussion on improving passenger screening. Experience, no matter its cause or origin, is the best teacher.

In addition to hearing about TSA's reaction to the Nat Heatwole incident today, we also have the opportunity to discuss recent government work to review TSA training, testing and supervision of passenger screeners.

The investigation by DHS IG found that TSA written tests for potential passenger screeners on the operation of explosive detention system machines were designed to maximize the likelihood TSA employees would pass, rather than ensuring that only competent and well-trained employees were responsible for passenger screening. In essence, they've been

"teaching to the test." More disconcerting was the DHS-IG's covert testing of passenger security screening operations. According to press articles, IG investigators were able to bring knives, a bomb, and a gun through Boston's Logan International Airport without being detected.

The GAO report cited deficient supervisory training programs and a failure to collect adequate information on screener performance in detecting threat objects. The report also cited the need for recurrent training for passenger screening, to ensure that screener skills are maintained and enhanced, as new security information becomes available. In addition, the GAO report found that Federal Security Directors, who are responsible for overseeing security at the airports, have expressed concern that they have limited authority to respond to airport-specific staffing needs. These needs include daily and seasonal fluctuations in passenger flow. We look forward to hearing more from GAO about their report during our second panel of witnesses.

TSA has stated that new procedures for passenger screener training and testing are in the works, including new written tests to replace the tests criticized in the DHS IG report. In addition, specific training courses designed for screener supervisors are being developed to improve screener performance. We are anxious to hear about these new changes.

There are currently five pilot program airports that use private companies to provide passenger screener functions. These private companies were responsible for developing and implementing training for passenger screeners prior to the federalization of passenger screeners by TSA and therefore have significant experience in the business of training,

testing, and supervision. We are pleased to have representatives from two of the private pilot program airports, the Kansas City International Airport in Missouri and the Greater Rochester International Airport in New York, on our second panel. We look forward to their testimony and hope to hear about their relationship with TSA, suggestions for improvements with the new federal workforce, and how the pilot program has worked with regard to passenger screener training, testing, and supervision.

The Committee is mindful that the holiday season has begun and that the traveling rush will inevitably result in longer lines at checkpoints. TSA has the immense task of maintaining adequate staffing levels for passenger screening over the next month and a half. At the same time, TSA passenger screeners will face additional pressure to process passengers quickly, despite the fact that they are not permitted to allow passengers into airport sterilized areas without resolving all possible threats identified in both passenger and carry-on baggage checks. But security measures at airports cannot be compromised. As travelers, we need to be prepared for rigorous security checks, and I hope that TSA can give us some advice today about how travelers can smoothly proceed through passenger screening checkpoints.

We look forward to a constructive hearing today – keeping in mind that no system is foolproof. In fact, keeping prohibited items off a passenger plane is but one layer of a multi-layered aviation security strategy, which includes hardened cockpit doors, additional federal air marshals, and armed pilots. The airlines have taken their own steps to increase the number of layers, by training their flight attendants in self-defense, for example. However, a chain is only as strong as its weakest link, and we are hopeful

that our oversight of TSA passenger screener training, testing, and supervision will improve overall aviation security.

Chairman TOM DAVIS. Is there any Member on the other side wishing to make an opening statement? Do any other Members wish to make opening statements?

We will proceed to our first panel, Steve McHale, Deputy Administrator of TSA. It is our policy here to swear in witnesses. If you will rise and raise your right hand.

[Witness sworn.]

Chairman TOM DAVIS. Welcome. Thank you for being with us. Before you go on, I am going to recognize Mr. Ruppersberger for just a quick statement. The gentleman from Maryland.

Mr. RUPPERSBERGER. Thank you, Mr. Chairman. I do represent BWI Airport, and one of the issues—I have to leave, unfortunately, to go to a funeral—but when TSA sits back and looks at really where we are, what we are accomplishing, it seems to me that what we have to analyze is the outsourcing, the continued outsourcing we are talking about. Is that as relevant as the actual training and making sure that we adjust the formula for all of our employees or contractors, the formula for what is safety? It has been said you can't have 100 percent, but we should try to reach that goal. That is really an issue I would like to put out.

Thank you, Mr. Chairman.

Chairman TOM DAVIS. Thank you very much. We will try to make sure that is answered.

[The prepared statement of Hon. C.A. Dutch Ruppersberger follows:]

Congressman C.A. Dutch Ruppersberger
Committee on Government Reform Hearing
"Knives, Box Cutters, and Bleach: A Review of Passenger Screening Training, Testing and Supervision"
Thursday - November 20, 2003
Remarks

Thank you Mr. Chairman. I thank you and Congressman Waxman for reacting so quickly to recent events and holding this extremely timely hearing. I represent the Baltimore Washington International Airport – a major American airport where 85 percent of the passengers start and end their trips at BWI. BWI continues to grow while the national average is down. So I certainly understand the challenges airports and agencies face in making commercial aviation safer for all Americans.

I appreciate that today is not about pointing fingers or playing blame games. This nation was rudely awakened to the ravages of terrorism just over two years ago and as a nation we continue to strive towards better safety and security.

The Department of Homeland Security and the Transportation Security Administration are still relatively new agencies and I believe GAO rightly commended TSA for juggling organization requirements with assessments, planning, and implementation.

These were not easy tasks, and statue held TSA to specific deadlines.

We are here today – not to criticize – but to assess where our passenger security system is and to identify ways to improve it. I have heard often that no security system can be 100 percent accurate and I can certainly appreciate that reality. But I would argue that 100 percent detection and accuracy should be our goal. The processes and systems including organization, hiring, training, testing, reviews and even possibly plans for outsourcing or contracting would be designed according to that goal. The processes and systems need to be in place first.

So while I am thankful for the GAO testimony and report released today, I am concerned that much of the focus appears to be on contractors and outsourcing for increased flexibility for privatization. Let me be clear. I am not opposed to the idea of outsourcing or privatization on principle. But regardless of who completes the work, I am not sure we have clearly defined what we mean by safe.

Recently I joined with Chairman Shays and other colleagues on the National Security subcommittee to introduce a bipartisan bill calling for national standards in homeland security. And I think the lack of national standards applies to TSA as well. We need to clearly define what we mean by safe, what our goals are, how we intend to achieve those goals – and ultimately what standards are necessary for passenger screener training.

As Acting Inspector General Clark Kent Ervin from DHS concluded in an August 2003 report on TSA training, there are two problems with TSA's overall training platform. First the protocol adopted maximized the likelihood that trainees would pass. As noted in the media and confirmed by DHS, final exam questions were identical to quiz questions. While that helped to certify trainers more quickly, I am not sure it made passengers safer.

Second and perhaps more worrisome, and I am quoting, "not a single question called upon a student to demonstrate a sufficient mastery of the class content to achieve the purpose of the training." Ervin determined this to be a critical defect in the TSA testing and certification process. I would have to agree.

My greatest concern is that we do not put the cart before the horse in solving the problems TSA faces in improving the passenger screening program. When one college student can wreak havoc and paralyze an entire commercial aviation system, there is most certainly room for improvement.

Commercial aviation is critical to national and global commerce. The travel industry is suffering enough. And we owe it to the American people to create the safest environment in which they can fly. I believe before we consider moving forward with further contracts and flexibility, we must ensure that the training platforms are sound. They must be based on best practices and sound training principles to fulfill agreed upon standards. That is not political rhetoric. That is simple common sense.

So what I learned most in preparing for this hearing is that we must start with TSA's adopted training protocol and make sure that it is sound. While improvements are being made, what about employees already trained by the old system? Do we go back and retrain? When will we fully deploy training programs for all employees and supervisors? When will we require a demonstration of mastery for certification?

I think we need to stop the cart for a moment and answer those questions first. Before we determine how effective the current training program is, I think recent events and investigations require us to ask if it is the best training program we can create and how we can improve it.

I look forward to hearing from the witnesses and learning more today through their testimony and our questions. Thank you Mr. Chairman.

Chairman TOM DAVIS. Also I want to recognize that the Metropolitan Washington Airport Authority is in the room, and other airport authorities are here, too, because I think we all share the concerns here and want to make sure we are up to snuff for the holiday season. As I said earlier, we are much safer today than we were a couple years ago, and despite what we see with some of the headlines at this point and the fact it is not a foolproof system, it is much improved.

Thank you very much. Go ahead.

STATEMENT OF STEPHEN McHALE, DEPUTY ADMINISTRATOR, TRANSPORTATION SECURITY ADMINISTRATION

Mr. MCHALE. Good morning, Mr. Chairman and Members. Yesterday was the second anniversary of the legislation that created the Transportation Security Administration, and I would like to take this opportunity to inform the committee of the major improvements in civil aviation security since the creation of TSA and of our plans for continuous progress in the months ahead.

Mr. Chairman, as you noted, I do have great confidence in telling you that the civil aviation sector is much more secure today than it has ever been, and it will be more secure tomorrow than it is today. TSA and its many partners, the airport authorities, the airlines and all of the vendors and contractors, our contract screening companies and others, have built an entirely new system of systems for aviation security that is reflected on the chart over here on the left, which I believe you also have copies of in front of you. This system of systems does not rely on any one component. There are many layers of our system of systems as illustrated on the chart, but we have to always recognize that we cannot rely on any layer to have a zero failure rate. If one layer is breached, we must have other layers that will have to be overcome as well, and that is our goal in building all the way through these rings of security.

Since September 11, our ability to gather, assess and share intelligence has dramatically improved. TSA keeps an around-the-clock intelligence watch tied to all national intelligence and law enforcement intelligence programs and maintains direct connection with TSA's field operations and with the security centers of major transportation stakeholders. That is perhaps the most important relationship, the to-and-fro of information between the private entities and the government. TSA's Transportation Security Coordination Center provides tremendous capability for prevention, response and mitigation. I am pleased, Mr. Chairman, that you had the opportunity to visit TSCC in person, and we invite other Members to tour those facilities as well.

We have made major improvements in perimeter security, conducted background checks on over 1 million air carriers and airport employees with access to secure and sterile areas of the airport, and implemented technological solutions to assist screeners with detecting threats. On September 11, there were only a few Federal Air Marshals. Today thousands are deployed on high-risk domestic and international flights. Every month Federal Air Marshals fly more missions than in the whole 20-year history of the FAM Service prior to September 11. Aircraft serving the United States are equipped with new, hardened cockpit doors. By the end of the fiscal

year, we expect to have trained and equipped thousands of pilots who volunteered for Federal Flight Deck Officer duty.

It may be valuable, Mr. Chairman, to step back and look at all that has been accomplished in a very short time. The chart on display tells a simple factual story of security screeners then and now. Before September 11, contract screeners had no national program of operating procedures or standards. Today Federal screeners and our private contract screeners meet consistent national protocols and must be annually recertified. TSA screeners receive much more robust and comprehensive training, and before September 11, screener attrition rates were 100 to 400 percent a year. Today, the current attrition rate at airports with TSA screeners is just 13.6 percent.

With all this in place, air travelers have good reason to feel more secure, but I must caution that threats to aviation still remain, and we must keep our security focused. Intelligence reporting tells us that commercial aviation remains high on the terrorists' target list. Last month alone we intercepted 564,000 prohibited items at the Nation's airports, including 1,900 box cutters and 41 firearms. We are surprised that we continue to find such large numbers of prohibited items carried by travelers and actively work with our partners in the aviation industry to continue to educate passengers.

As you are aware, there have also been highly publicized incidents of smuggling prohibited items onto aircraft. These incidents are the subject of ongoing investigation. But let me be clear that TSA is well aware that our system has vulnerabilities, and as we identify them, we take swift action to address them.

TSA has changed the procedures at its Contact Center so that e-mail, telephone calls and other communications are filtered for security content, reviewed by a security analyst, and, when appropriate, transmitted to the TSCC and other units for action. We have changed procedures throughout TSA so that all personnel are prepared to identify, document and report potential threat communications.

TSA recently strengthened the preflight inspection requirement for passenger cabins, increasing the thoroughness of the search. In addition, the airlines are required to contact the local Federal Security Director [FSD], and local law enforcement immediately if anything suspicious, dangerous, or deadly is located.

TSA conducts an aggressive covert testing program to challenge screeners to detect threat objects at screening checkpoints and in checked baggage using simulated terrorist threat devices and techniques based on the latest intelligence. We are conducting these tests at three times the rate of the old FAA Red Team testing. We use the results of these tests to provide specific feedback to screeners and FSDs at airports. The results also drive change and improvement in our standard operating procedures, training and technology. We are constantly increasing the sophistication of these tests to ensure that our screeners are prepared to counter evolving threats to aviation security.

If our Red Teams do not get items through the checkpoints, they are not trying hard enough. We challenge them to try to get items through the checkpoint, and then we challenge our screeners to try

to stop them from getting through. It is a constant push and tug in the testing process to constantly improve our work force.

TSA conducted a screener performance improvement study to determine the root causes for deficiencies in screener performance found in covert testing. Well before the recent incidents, TSA was already preparing a plan to enhance screener performance. The nine elements of our short-term screening improvement plan are highlighted on this chart that is being displayed now.

Under TSA's plan, we will increase the number of unannounced covert tests at airports to assess system and airport-specific screening performance. Airports with below-par performance on covert tests will receive special training. Teams of industrial engineers, trainers, performance consultants and technology and management experts will work with the FSDs to design and implement solutions.

We are also enhancing recurrent screener training and supervisory training. Recurrent training is needed to maintain and enhance the skills of screeners, particularly in the area of x-ray image interpretation, the search of persons and the inspection of property. Supervisory training will enhance leadership skills in our work force and provide the advanced technical skills needed to better oversee the screening process and resolve alarms.

With your permission, Mr. Chairman, I would like now to show you a 30-second clip from one of an exhaustive series of videos we are going to be using in training.

[Videotape played.]

Mr. MCHALE. A major initiative to improve screener performance and accountability is enhanced through our Threat Image Protection [TIP] system. TIP superimposes threat images on x-ray screens during actual operations and records whether or not screeners identify the threat object. This tool is excellent for evaluating the skills of each individual screener so they can focus directly on the areas needing skill improvement and taking disciplinary action where necessary. By regularly exposing screeners to a variety of threat object images, TIP provides continuous on-the-job training and immediate feedback. Today we have over 1,400 TIP-equipped x-ray machines in place around our Nation's airports, and every checkpoint lane will be equipped with TIP by the summer of 2004. TIP and other similar testing ensures that our screeners have the right set of practical skills and are an appropriate complement to our multiple-choice testing, which ensures that screeners are well-versed in procedures and process.

Technology is an absolute necessity in detecting threats. TSA has a robust research and development program to help make our operations more effective, more efficient, less time-consuming, and less costly. Extensive cooperation with the private sector in the development of technology is a hallmark of our program. TSA is testing two explosive trace detection portals that analyze the air for explosives as passengers pass through them. We are continuing to work on identifying the next generation of explosive detection equipment for use in screening carry-on and checked baggage.

In the aftermath of September 11, the screener work force was Federalized to reassure the traveling public and to provide uniformly high training and standards for screeners by leveraging the

resources of the Federal Government. TSA's private screening pilot program provides a basis for comparing the effectiveness of both Federal and contract screening. In either case, TSA will continue to closely supervise the screening operations and ensure that uniform standards for screeners and equipment are maintained. We also are working with the contractors to solicit creative and innovative ideas for security. We have not denied any formal request for additional operational flexibility that is permitted by law.

TSA also is moving forward toward implementation of the second generation of Computer-Assisted Passenger Prescreening [CAPS] II. CAPPS–II will greatly enhance our ability to identify terrorists and other high-risk individuals before they board commercial airplanes. It will help us focus our resources on those that pose a higher risk to aviation security than the general population, while reducing unnecessary screening for low-risk passengers. We can and will achieve this benefit while incorporating robust privacy protection measures for the traveling public.

Another area in which we are making significant steps forward is in air cargo authority. Just this week Secretary Ridge announced the first building blocks in TSA's comprehensive Air Cargo Strategic Plan. Air carriers will be required to randomly inspect cargo on passenger aircraft and in all cargo planes on both foreign and domestic flights in the United States.

As we build new and strengthen existing security measures, we must always keep in mind the customers, particularly the traveling public, and as we start this busy holiday season with the pickup in air travel, TSA is working hard to minimize the long lines we normally see this time of year. Air carriers and airports have been very cooperative in pre-holiday planning to keep lines moving as quickly as possible. Airport and airline personnel are stepping up to assist in non-certified positions in airports when needed so that certified personnel can focus on screening. Vendors and concessionaires are working with us to schedule airport deliveries at off-peak times.

But, Mr. Chairman, as you noted, travelers can avoid the secondary screening process by preparing for takeoff and save 3 minutes by placing loose items in a larger carry-on, taking children out of strollers as they approach the checkpoint, and by removing coats before they go through a checkpoint. TSA has worked hard to reassure travelers by creating many hurdles in the path of a potential terrorist, and we are continually evolving our security systems to ensure we are always a step ahead.

Mr. Chairman, I would be glad to answer any questions you and the committee might have.

[The prepared statement of Mr. McHale follows:]

DEPARTMENT OF HOMELAND SECURITY

STATEMENT OF

STEPHEN J. MCHALE
DEPUTY ADMINISTRATOR
TRANSPORTATION SECURITY ADMINISTRATION

ON CIVIL AVIATION SECURITY

BEFORE THE
COMMITTEE ON GOVERNMENT REFORM
UNITED STATES HOUSE OF REPRESENTATIVES
November 20, 2003

Good morning Mr. Chairman, Congressman Waxman, and Members of the Committee. On behalf of Admiral Loy, I am pleased to appear before you today to discuss the advances in civil aviation security made by the Transportation Security Administration (TSA) and recent events involving the smuggling of prohibited items aboard aircraft.

TSA was established just two months after the September 11 attacks on our Nation when, on November 19, 2001, President Bush signed the Aviation and Transportation Security Act (ATSA). TSA is now a proud part of the Department of Homeland Security (DHS). With guidance and direction from the Border and Transportation Security Directorate, TSA and its sister agencies, the Bureau of Customs and Border Protection (CBP), the Bureau of Immigration and Customs Enforcement (ICE), the Bureau of Citizenship and Immigration Services (CIS), and the Federal Law Enforcement Training Center (FLETC), are working together to strengthen security at our borders and in our transportation systems.

TSA and its many partners have built an entirely new aviation security system that offers significantly higher levels of security than were in place in September 2001. We have built a system of rings of security—a system of systems that does not solely rely on any one component. We continuously gather as much information as possible about the threats, vulnerabilities, trends, and conditions of the aviation system and its environment. We use this domain awareness to prioritize and direct resources and take protective action. TSA's Transportation Security Intelligence Service receives, assesses, and distributes intelligence on threats to transportation and operates an around-the-clock intelligence watch tied to all national intelligence and law enforcement intelligence programs. It maintains direct connections with TSA's field operations and the security centers of major transportation stakeholders. Airport access controls and airport perimeter security are strengthened, and we have 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. Highly trained, qualified personnel screen every bag and every passenger 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. TSA-certified canine teams perform multiple tasks throughout the entire airport environment, including screening checked baggage, searching unattended bags, searching vehicles approaching terminals during increased threat levels, screening cargo on a limited basis, and responding to bomb threats. The number of Federal Air Marshals has increased from just a handful on 9/11 to thousands today, and they are now deployed on high-risk domestic and international flights. Commercial aircraft serving the U.S. are equipped with new, hardened cockpit doors. TSA's Federal Flight Deck Officer program trains, equips, and deputizes pilots who volunteer to defend the flight decks of passenger aircraft as the last line of defense. By the end of FY04, at the current pilot application rate, we expect to have trained thousands of pilots who have volunteered for the program and met the initial background requirements.

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 inherited a 30-year-old passenger-screening system designed to detect obvious weapons such as guns, hunting knives, and grenades, and has transformed it into a system that also finds much smaller and less obvious threats. We take pride in the professionalism and diligence shown by TSA screeners every day in their efforts to ensure the safety of the traveling public. Since February 2002, TSA has intercepted more than 1500 firearms and more than 54,000 box cutters. Nevertheless, there is no such thing as a zero failure rate for passenger screening. The individual components that comprise our rings of security are filters; they are not guarantees. Taken together, the combination of security measures compensates for the potential weaknesses of a particular component.

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. Our daily intelligence reports frequently contain information on new methods that terrorists might employ against the transportation security system. We also receive daily reports from airports on secreted prohibited items and other suspicious items that our screeners discover. 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 increased by 28 percent 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, a sword hidden inside a cane, and a gun secreted in a child's teddy bear.

On October 16, 2003, a maintenance technician for Southwest Airlines found two types of prohibited items, liquid bleach secreted in a suntan lotion bottle and boxcutters, as well as molding clay, matches, and an anonymous note in the rear lavatory of an aircraft in New Orleans. That night, similar items were found on another Southwest aircraft. When notified, TSA was able to initiate a record search quickly and link these situations to an email that TSA's Contact Center had received in September. The email included the sender's identity and details of his actions but did not include an overt threat. He was identified in less than 12 hours and interviewed in less than 20 hours from the time of notification to TSA. In those first 12 hours TSA also contacted the principal security officer of every U.S. air carrier and issued a directive that they perform fleet-wide security inspections within 24 hours.

Because the circumstances surrounding this incident are now the subject of a Federal investigation, it would be inappropriate for me to provide further information in this setting. Instead, I will focus on the steps that TSA has taken to prevent it from reoccurring.

First, the channel through which TSA received the email needed additional attention. TSA's Contact Center has been the focal point for receiving comments on travelers' experiences in screening and for reporting lost or damaged property, but not for receiving security alerts. The Contact Center receives an average of more than 5,000 telephone calls and e-mails each week, the vast majority reflecting the types of concerns noted above. The email that TSA received through this channel was not viewed as a threat, but clearly it should have received priority treatment as a potentially serious message involving security information and illegal activity.

TSA has swiftly changed procedures at its Contact Center and throughout TSA. Contact Center electronic mail, telephone calls, and other communications are now filtered for security content, reviewed by a security analyst, and when appropriate, transmitted to our Transportation Security Coordinating Center and other units for action. Contact Center personnel are trained each month on how to identify potential security violations, threat information, and criminal activity conveyed through telephone calls or other means. In addition, all TSA employees and contractors have been given specific protocols to follow in identifying, documenting, and reporting potential threat communications.

We know that there is more to do. Well before this recent episode, TSA was assessing its vulnerabilities and moving forward on a plan for screener improvement. TSA conducts an aggressive covert testing program that challenges screeners to detect threat objects at screening checkpoints and in checked baggage using simulated terrorist threat devices and current techniques. Between September 2002 and October 2003, our Office of Internal Affairs and Program Review (OIAPR) conducted 847 checkpoint and 2,737 airport security access tests, as well as computer assisted passenger prescreening (CAPPS) and checked baggage tests at 107 airports. We conduct covert testing at over three times the annual rate of the old FAA "red teams," and our testing uses more difficult, realistic testing situations. Although TSA cannot discuss the results of our tests in detail in this setting, results have shown an improvement of approximately 10 percent

from September 2002 to August 2003. This progress is particularly significant because the difficulty of the tests has increased over the past year.

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 its own covert tests and tests performed by the DHS Office of Inspector General (OIG), in addition to the OIAPR tests. This report notes the continuing need to improve screener performance and to implement performance measures to determine the effectiveness of screening operations. We concur with that finding.

In July of this year, TSA conducted a Screener Performance Improvement Study to determine the root causes for deficiencies in screener performance. After identifying the desired level of screener performance, we gathered data from multiple sources to determine the actual, current level of performance and the root causes for the gap between desired and actual performance.

Based upon the Screener Performance Improvement Study, TSA identified an array of specific follow-up actions. These enhancements are now being implemented under TSA's Short-Term Screening Improvement Plan outlined below.

1. Increased Federal Security Director (FSD)[1] Support and Accountability. Under TSA's plan, airports with below-par performance on covert tests will receive special attention. Teams of industrial engineers, trainers, performance consultants, and technology and management experts will identify the causes for poor performance at these airports and work with FSDs to design and implement solutions. Follow up will include additional covert testing and FSD accountability for any continued performance deficiency. We will also create incentive programs to encourage top performance.

2. Enhanced Training for Screeners and Supervisors. National, validated skill standards for all screeners form the foundation of an integrated system for hiring, training, certifying, and measuring performance. All screeners must demonstrate the qualifications, knowledge, skills, and aptitudes necessary to meet Federal standards and successfully perform as a transportation security screener. They receive a minimum of 40 hours of classroom instruction and 60 hours of on-the-job training. Screeners are subject to periodic proficiency assessments and unannounced performance testing. They are made aware of new threats and methods of concealment.

Screeners who fail any operational test are removed from their screener duties and must complete remedial training prior to returning to duty. Current guidance to FSDs on remedial training is that each screener must review all pertinent sections of the standard operating procedures (SOP) and Basic Screener Training modules or the appropriate recurrent training modules.

---

[1] The Federal Security Director (FSD) is the senior TSA security official responsible for aviation security operations at one or more airports. TSA currently has 159 FSDs responsible for over 400 commercial airports. Our FSDs come from many security related occupations including aviation or other transportation security disciplines, the armed forces, as well as federal, state, and local law enforcement officials.

Maintaining a high level of screener proficiency requires constant diligence. Two important elements of TSA's plan for screener improvement are recurrent screener training and supervisory training. Recurrent training is needed to maintain and enhance the skills of screeners, particularly in the areas of x-ray image interpretation, the search of persons, and the inspection of property. Supervisory training will enhance leadership skills in our workforce and provide the advanced technical skills needed to adequately supervise the screening process and resolve alarms.

Our recurrent training program is under development, though two modules have already been delivered to the field. In the meantime, FSDs have been encouraged to use the training modules of the Basic Screener Course to address specific recurrent training needs. Many have done so, and others have developed their own supplementary training. Also, screeners are required to undergo weekly x-ray image interpretation training using state-of-the-art computer-based training. FSDs at airports have received the first of a series of screener performance improvement videos and more than 350 courses will be available via our new Online Learning Center or through access to compact discs. We are also certifying over 800 screeners and training coordinators to teach various topics at each airport.

Recently, approximately 500 of TSA's 3600 screener supervisors completed the U.S. Department of Agriculture (USDA) Graduate School Introduction to Supervision course. This course is being modified to make it airport screening specific and will be introduced nationally this December. Further tailoring of the course has begun so that its content better meets the needs of screening supervisors, and we expect this enhanced course will be offered in March 2004. Our plan calls for all supervisors to complete supervisor training classes in six months.

All screeners must meet annual recertification standards, which require passenger screeners to pass an Image Certification Test, SOP Job Knowledge Test, and Practical Skills Demonstration, and require 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 2003-2004 began on October 1, 2003, and will run through March 2004. Screeners that fail to pass any of the recertification components will be terminated. As part of our recent rightsizing effort, approximately 28,000 screeners completed portions of the proficiency testing. We will consider successful completion of those tests to be a part of the annual recertification.

3. Increased Frequency of Internal Affairs Covert Testing. To help improve screener performance, TSA will increase the number of unannounced, covert tests at airports across the Nation to assess system and airport-specific screening performance. OIAPR's testing plan is designed to test all of the airports during a three year period with Category X airports tested annually, Category I and II airports tested biannually, and contract

screener pilot[2] airports tested semiannually. Additional testing may be performed by each FSD.

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, and/or improving technology, as appropriate. The covert tests serve as one of many indicators of screener performance. They 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.

4. Human Performance Improvements. A key element to improving screener performance is to understand the impact of screening tools, technologies, operating procedures, and environmental factors on screeners' abilities to perform their tasks. We are conducting studies to determine the causes and solutions for individual screener errors, team errors, communications breakdowns, and possible technology and procedural bottlenecks. These studies will help establish baselines, enabling us to evaluate and measure the potential impact of new technologies and procedures before they are implemented.

5. New Screening Technology. Technology is an absolute necessity in detecting threats. TSA has a robust research and development program and works closely with the DHS Science and Technology (S&T) Directorate to develop and deploy technology that will help make our operations more effective, more efficient, less time consuming, and less costly. TSA has a state-of-the-art research laboratory, the Transportation Security Laboratory, located in Atlantic City, New Jersey. 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. 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, but will not consider deployment on any of these technologies until sufficient safeguards are put in place to ensure the protection of passenger privacy.

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 in smaller amounts than are currently established in our certification standard

[2] TSA is operating a pilot program at five airports using private screeners that must meet all TSA eligibility, training, and performance requirements and receive pay and other benefits equal to those of TSA screeners

and will occupy a smaller footprint at already overcrowded airports. TSA is looking at new applications of X-ray, electro-magnetic, and nuclear technologies to better probe sealed containers for materials that pose a threat.

6. Complete 100 Percent Threat Image Projection (TIP) System Deployment. Another major initiative to improve screener performance is the implementation of an enhanced version of the TIP system. TIP superimposes threat images on x-ray screens during actual operations and records whether or not screeners identify the threat object. This tool is excellent 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 and remediation. TIP allows supervisors to closely monitor screener performance and improvement.

TSA is expediting the replacement of approximately 1,800 conventional x-ray machines with TIP-ready x-ray machines (TRXs). We now have over 1,300 new TRXs in place.

Our TIP system is an improvement over the predecessor FAA system in several respects. The Federal Aviation Administration (FAA) created a library of only a few hundred images, which when shared with screeners, eliminated any real test value. In contrast, 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, we will primarily rely on using the limited library as an on-going training tool. Once TSA has the expanded TIP library on all TRXs in place, we will collect and analyze the data. The analysis will allow 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 develop and implement appropriate skill enhancement strategies.

7. Expedite IT Connectivity to Checkpoints and Training Computers. TSA is taking action to deliver connectivity to all TSA locations within airports across the country. This will provide the capability for continuous training, including real-time training on current threats; greater capacity for monitoring TIP performance; connectivity with checked baggage areas; and a foundation for planned implementations of additional administrative, surveillance, CAPPS II, and other security enhancements. Unfortunately, the screening system that TSA inherited did not include this key element, and it has been both costly and time consuming to get where we would like to be in this area.

8. Update Aviation Operations Policy, Procedures, and Practice. We are updating our policies, procedures, and practices based on the lessons we have learned over the first year of Federal screening. Aviation travel is dynamic, demanding an agile system of

reevaluation and response. This process will be ongoing based on field experience and new intelligence.

In addition, TSA, working with the DHS S&T Directorate, will begin a comprehensive review of the civil aviation security system now that two years have passed since the enactment of the Aviation and Transportation Security Act and over twelve years have passed since the enactment of the Aviation Security Improvement Act of 1990. This is part of our constant evaluation of the security measures we have put into place, and now we have time to consider other approaches to aviation security that may be available to us.

9. Improve Workforce Management Scheduling and Staffing. To manage our workforce most effectively, we are exploring new methods and tools to allocate our workforce resources. We are paying close attention to human performance issues, technology limitations, and scheduling needs. There are tradeoffs that must be carefully considered such as the potential for a decreased performance level during long shifts. Recognizing that most airports have peaks and valleys in daily passenger activity, particularly at smaller airports, we are converting the workforce to a mix of full- and part-time screeners tailored to each airport. This approach will provide a better match of screener staffing with actual passenger levels at any given time.

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 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. TSA is assessing if and how it will expand contract screening and to help us make these decisions recently awarded a contract to perform a rigorous assessment of the screening pilots. We will provide a program strategy and plan well before November 19, 2004.

In addition to improving screening at airports, TSA is working hard to improve airport perimeter surveillance and protection. 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. We are currently focusing on four key areas and related technology projects: (1) security of access control through intended entry points; (2) security surveillance of perimeter areas; (3) improved security response capability to intrusions and security breaches through automated decision aids; and (4) oversight of industry compliance with current security requirements. TSA has collected and catalogued information on more than 300 applicable security technologies that include: biometrics, detection and prevention devices, surveillance technologies, and proximity sensors. Testing and evaluation of these and other technologies will be performed by

TSA in partnership with airport operators who have volunteered to be participants in a pilot program.

To ensure and improve its organizational effectiveness across the board, TSA has established performance planning and reporting mechanisms and continues to use these systems to collect data to monitor our progress toward achieving its goals. By managing this data in a central repository, TSA can assess equipment and personnel needs and status and make tactical decisions based on performance. Our Performance Measurement Information System (PMIS) was developed to capture basic performance measures at the airports on a daily basis and is continually being updated to reflect new requirements. TSA can proactively capture and analyze data on its security operations and adjust operations to achieve desired performance goals. Random and routine inspections, plus program evaluations, are also conducted to supplement the information captured by PMIS.

TSA is working to finalize and implement a set of new screener and screening system performance measures. TSA has already created the Customer Satisfaction Index for Aviation Security Operations (CSI-A), a succinct measure of our success in providing world-class customer service. The CSI-A is based on four inputs: passenger surveys at airports, a national poll, complaints and compliments made at airports about security, and complaints and compliments received at our TSA contact center. Data from each of these four inputs are scored and aggregated to form the CSI-A.

TSA is well on its way toward implementation of another important tool in its system-of systems of security, the second-generation Computer Assisted Passenger Prescreening System (CAPPS II). We appreciate the opportunity that we had to testify on the CAPPS II program before the Subcommittee on Technology, Information Policy, Intergovernmental Relations, and the Census this past May. CAPPS II will greatly enhance our ability to keep terrorists off of commercial airlines without disturbing the efficient flow of passengers or compromising their privacy. It will also help us focus our screening resources where they will be used most effectively. CAPPS II is intended to identify terrorists and other high-risk individuals before they board commercial airplanes. CAPPS II will conduct a risk assessment of each passenger using national security information and information provided by passengers during the reservation process—including name, date of birth, home address and home phone number—and provide a "risk score" to TSA. The "risk score" includes an "authentication score" provided by running passenger name record (PNR) data against commercial databases to indicate a confidence level in each passenger's identity. 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.

In developing CAPPS II, TSA is very mindful of the rights, liberties, and freedoms that define our Nation and differentiate our society from those who seek to harm us. CAPPS II is being designed and will be built with the explicit requirement that privacy protection not become a cost of increased aviation security. CAPPS II is undergoing a rigorous course of testing and will not be implemented until it has successfully passed

this test phase. As part of its ongoing dialogue with the public on CAPPS II and related issues, DHS 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. The Notice requested public comment, and the closing date for submission of comments was September 30, 2003. We are now in the process of reviewing the many comments we received. TSA is also cooperating fully with the U.S. General Accounting Office (GAO) so that GAO can issue the report called for in the Department of Homeland Security Appropriations Act, 2004, by February 15, 2004.

Cargo security on passenger aircraft is a concern for all of us engaged in transportation security. This week, Secretary Ridge announced important new steps in our efforts to have the best possible protection for air cargo. TSA has issued security directives to require random inspection of air cargo and to require foreign all-cargo air carriers to comply with the same cargo security procedures that domestic air carriers must follow. These actions are building blocks in a comprehensive Air Cargo Strategic Plan that uses a threat-based, risk managed approach. The Plan is based on recommendations of working groups of TSA's Aviation Security Advisory Committee, as well as recommendations from the GAO and the Department of Transportation's Office of Inspector General.

With the holiday travel season upon us, TSA will work hard to minimize the long lines that we see normally this time of year. Travelers are another critical partner in aviation security, and they can do their part by conscientiously avoiding carrying prohibited items and following tips to help security lines flow more smoothly. As we did last year at this time, we are carrying out a major public outreach effort for air travelers.

TSA appreciates this first opportunity to appear before the full Government Reform Committee to discuss its broad strategy for aviation security and to explain its strategy for improving screener performance. Since the tragic events of September 11, 2001, we have worked very hard and have come a long way in answering the Nation's call to improve the civil aviation security system. We better understand the threats to security and have dramatically improved our capability to share information on threats. We have built a highly skilled and professional screening force and greatly enhanced security technology at airports. We know that we must be alert for new threats and must continually assess and revise our systems to meet these threats. We have all learned a great deal very quickly, and we are using every tool at our disposal to drive toward excellence.

I will be happy to answer any questions you may have.

Chairman TOM DAVIS. We have a series of three votes. I will try to get a couple out of the way. I am going to start with Mr. Platts.

Mr. PLATTS. Thank you. I appreciate your testimony and the testimony you provided and the challenge your agency has. I do realize it is one that is pretty formidable, and it is an ongoing effort to try to keep up with the times of what the threats are.

One of your statements, if you could expand on it, jumped out at me. In the last year and a half, 1,500 firearms, 54,000 box cutters. What is defined as a box cutter? What is included in that 54,000? That just seems like a staggering number, given the box cutters being used in the terrorist attacks.

Mr. MCHALE. There are two common kinds we find. Usually it is either a handle with a fixed razor blade in the handle for slicing, or one with a retractable razor blade. But that is the kind of implement we regard as a box cutter. It has a razor blade in it usually.

Mr. PLATTS. Is there a common explanation of why somebody has this, given the times we are in?

Mr. MCHALE. That is a question I ask all the time. The answer is almost always, "I forgot I had it." A lot of people actually do carry box cutters as an alternative to a penknife with them. A lot of people carry it for work and other things. They are used to carrying it all the time. So they do say, and I think perhaps often truthfully, that they forgot they had it. It does strike me, given all the reporting on September 11, given everything that has been going on, as remarkable that people getting on an airplane don't think about what they have in their pocket.

Mr. PLATTS. Is there any consideration at TSA of working with the airlines, when you make a reservation, saying, "Is there anything else we can help you with today," of having a one-sentence reminder that knives, box cutters, guns—a pretty obvious statement to me, but apparently 54,000 occurrences, it is not as obvious as I guess I would think it should be.

Mr. MCHALE. The airlines and the airports have been very cooperative with us. They do help us with announcements with the public address system, placing of signage. The airlines are generally a little concerned about additional statements to their interaction with passengers just because of time considerations. But they have been very cooperative with us in trying to find ways to communicate this message in a way that works for them as well as us.

Mr. PLATTS. I thank you for your testimony and the efforts of your Department and agency.

Chairman TOM DAVIS. Thank you very much.

Mr. Kanjorski, we have 6 minutes in the vote.

Mr. KANJORSKI. I represent the Wilkes-Barre-Scranton airport. Recently you had a RIF announced where you are reducing 47 full-time employees to 26 employees, 2 full-time and 24 part-time. I don't know how we expect 24 people to live on 20-hour-a-week work, so it seems to me the quality and the availability of those workers is going to fall precipitously. Most of all, it sends an indication that this is the type of airport that a terrorist should really go to because the chances are that they are going to have less than professional screening capacity and a significant turnover in em-

ployees, if you are going to have 24 or 26 as part-time, 20-hour-a-week employees.

The second part of my question is, I understand you are contacting programs to get additional screeners, one just at a kiosk outside of northern Virginia here, and it seems to me if you are RIFing trained employees now at some airports, you should have more than enough to relocate them to new facilities. Why isn't this happening?

Mr. MCHALE. We have been reducing the number of screeners following the direction from the Congress in our appropriations act. But we have—just to answer your second question first, we actually have quite an aggressive program for relocation, giving displaced screeners the first opportunity to apply for vacancies at different airports around the country. Obviously, this involves moves, and we do find a lot of people don't want to do that. They are committed to the area in which they live. But where an employee is willing to relocate, we want to work with them to achieve that.

On the first part, we actually have found good quality people who are willing to work part time. It fits into other schedules. So we haven't had a quality decrease as we have gone out to seek part-time screeners.

The big question and the hard question for us really throughout the last 6 months as we have gone through this downsizing, rightsizing, at some airports it was actually an increase, but largely across the country it was a decrease—the big challenge we have had is working with our screeners and explaining to them why we are going to a lower level.

I don't know the details of Wilkes-Barre-Scranton. I can say, though, that at a number of regional airports there are often large gaps during the day in which there are not flights. Often there are a couple of morning flights and a couple of evening flights, maybe one at lunchtime, one or two, whatever it might be. The problem with that is with full-time employees, we often have them literally waiting for 2 or 3 hours for another plane to come in and really nothing for them to do in that time. So we have looked at split-shifting and done that at some places where they work 2 or 3 hours in the morning or 3 or 4 hours in the evening. We tried to accomplish that, but the trouble with the peaks and valleys, just the nature of the aviation industry, is we need people for 3 or 4 hours at a time. That is why part-timing works better.

Mr. KANJORSKI. Could you give me a report back, particularly on the Wilkes-Barre-Scranton Airport and its conditions?

The last situation, these 24 part-time employees, are they going to have any benefits, or by going to part time are they losing benefits and health care and all of that?

Mr. MCHALE. They will have benefits.

Mr. KANJORSKI. They will maintain their benefits?

Mr. MCHALE. That is right. They will be proportionate to the number of hours they work, but they get their benefits. In terms of retirement, they accumulate that.

Mr. KANJORSKI. And health care.

Mr. MCHALE. And health care.

Chairman TOM DAVIS. Thank you very much. We are going to recess. We will be back in about a half hour.

[Recess.]

Chairman TOM DAVIS. We will start the questions with the gentleman from Florida, who is, as you know, very involved with this in his other committee assignment as well and has taken a leadership role in this. Mr. Mica.

Mr. MICA. Thank you, Mr. Chairman; and I'm glad that you're conducting an oversight hearing on these issues that are so important to the flying public. Let me just make a couple of comments, and then I'll sort of transform this into a question.

But, as you may know, Mr. Chairman, I asked the GAO to conduct a preliminary—well, to conduct a review of some of the progress that we've made with our airport screening force, this small army that has been put together. The initial response was critical. Some of the public comments are in this—some of the nonpublic comments to the performance are classified, but I can tell you that the system is far from foolproof, as is demonstrated by the college student.

What concerns me is two things: first, that we have not made much progress, other than hiring an army of personnel, in really being able to detect threats and secure the safety of our passengers.

I see Mr. McHale is here, and I brought sort of a little array of some common items. What I want to do for the committee and for the record is to illustrate that this system that we have is easily penetrated. While part of the responsibility for not implementing steps to deal with this lies with TSA, part is also the responsibility of Congress.

The technology that we have at our airports today is basically, for the most part in passenger screening and screening passenger luggage, is 1950's x-ray technology. Here's a plastic box cutter. That equipment will not detect this plastic box cutter. If it had a blade that was non-metallic, the blade could be put in some other recess. So it's easy to get through.

I put $50 million in the original TSA legislation authorized and, unfortunately, Mrs. Murray from the State of Washington—Senator—diverted part of that to a project for her State. So it wasn't TSA's fault to not develop technology that would detect this type of box cutter, which you can—I could still take this through Washington National or any airport right now. Their technology will not detect this.

Then if you take bleach, common household bleach, and I put it into this—I can use that to—as a weapon, carry it on any aircraft, and it is not detectable, use it against aircraft personnel. There's no equipment that we have that will detect that. This looks like a bottle of wine, but I've actually filled it with flammable material; and, of course, if I had a handkerchief, it makes a great fuse. Here's—while we ban—we've confiscated things like fingernail clippers, here's a lighter that can create an incendiary device to do a great deal of damage, if not take down an air craft.

We put $70 some million in for advanced technology, $75 million, I believe it was. TSA turned back all but $62 million in the fiscal year that just ended for salaries. So we don't have equipment or technology that will really look at any of these threats.

And I haven't even gotten into explosives. I didn't bring any Play-Doh that would simulate explosives. But we have almost no technology that would detect explosives strapped with duct tape around a passenger such as Richard Reid did, but he did it very expertly, concealed in the heels of his shoes. So I think that this young man, while he may have violated the law, did hopefully awaken us to the need to move forward.

Now the good news is there's some $200 million to get to the next step of technology that will analyze matter and will also determine what is in the contents, if it's liquid or other material. Also, there is technology I've seen that will deter—can look at shapes and other dangerous items. So we're far behind. We've created a multibillion dollar mirage. You can hire 200,000 screeners, they can be private or they can be public, and we're still at great risk. The good news is we have secured cockpit doors. We have armed marshals on many of the aircraft, and we've also allowed pilots to be trained to defend their aircraft and passengers.

But we need to go much further. This isn't—this little display is just a small sampling of what can be done, and we know terrorists as recently as this morning have shown that they have very destructive intentions. Why this is important is that if we take another hit with a commercial aircraft it not only will devastate the aviation industry but also devastate our economy. So TSA has done a good job in ramping up an army. They have not done a good job in creating the technology necessary to detect these threats.

So the only question I have, Mr. McHale, is how are we coming on the development of technology to deal with some of these threats?

Mr. MCHALE. I agree with you completely that the technology we're using is somewhat better than September 11 but not a lot. It is the same type of technology. We've replaced all the metal detectors with the latest generation, but it is still the pre-September 11 x-ray and metal detection technology; and it is a technology that was developed to detect firearms, large bombs, large knives. We're trying to use it—and we use it with some success—but we're trying to use it to detect much smaller items today. We do need to improve the technology and improve the equipment that we have for our screeners.

We've made, actually, I think, substantial progress in the development of explosive detection portals that will detect the explosive vapors in the air around passengers as they pass through the portal. I'm hoping that we will be able to deploy some of those in a prototype to try to test them out in the operational phase in the not-too-distant future and then move forward to getting them throughout the system. That will certainly help with the belt of explosives and that kind of thing that a passenger might carry through on their person.

Some of the technology similar to that could be available also to help us with explosive detection in carry-on baggage. We're looking at that. We have problems with sizing that for the space and making it operational. The technology is there. Making it fit into the operational environment and the speed with which we have to deal in the operational environment, the equipment is just not there yet.

We have some very promising technology that we may deploy very shortly that will help us with one of the items that the General Accounting Office displayed to your committee, sir, and will help us actually look inside some of those items without having to remove them from the passengers. So that may be very helpful to us.

We are constantly trying to figure out how to match the technology to the emerging threat, and you are correct that the threat changes, and the threat has changed dramatically in the last couple of years, and we need to continue to find new technologies. Perhaps the biggest challenge we do have—there are a lot of good ideas out there, but getting them operationalized into the airport setting is often a really big hurdle.

Mr. MICA. Well, again, Mr. Chairman, I'm very concerned about the lack of progress. When they turned back this year some $60 plus million of $75 provided for getting us to the next stage of technology, using that on personnel is not acceptable. We will never address the terrorist threat. You cannot deploy enough screeners and individuals to deal with this threat unless you have the latest technology.

Finally, one of the things that disturbs me in this incident—and I'm glad again that we have a chance to look at this—is this young man also notified TSA, and TSA failed to act. Now one of the things that we put in the TSA bill was we—and as far as our screening employees and others involved in this, we did not protect them with the protections of Title 5, Civil Service protections. So I'd like to know, has that—have those individuals been held accountable or have they been elevated to some higher position, which is sometimes the custom in our Federal agencies? But there are specific individuals who had information about the threat or the actions of this individual and did nothing about it. What's the status?

Chairman TOM DAVIS. Can I just interject there? Your time's up, Mr. Mica, but we recognize your role over on the other committee on this. This may be something, because it is a personnel action, that you might want to communicate with him individually on. I think you need to know that, but I——

Mr. MCHALE. I'd be happy to do that.

Chairman TOM DAVIS. All right. Go ahead. Any way you want to do it. If you feel comfortable——

Mr. MCHALE. I will communicate with you about the personnel actions taken off the record. But what I can say is that we did set out, one, to develop a system. We get a large number of e-mails into that system. It can take us some time to review those e-mails and respond to them. So we've developed a system to filter out and send up for review immediately any kind of threat information that we find. So we send that immediately to an intelligence analyst and security analysts to take a close look at to identify the threat if there is threat information in that and then to refer it to our operational side to take immediate action, including referral to the FBI or whatever else we have to do to deal with it. It was obviously a major concern to us when it came to my attention on October 17 that we'd had that e-mail since September 15, and we immediately took steps to correct that. We've instituted training both for the

Contact Center—they've all been trained—and also for all TSA employees, not only to recognize potential threat information but to act on it and to know how to act on it and where to send it to. The Contact Center was relatively new. It was set up for consumer affairs, but it should have recognized and should have been set up to recognize that it could receive that kind of threat information, and we've taken steps to address that.

Chairman TOM DAVIS. OK. Thank you.

Mr. MICA. Thank you, Mr. Chairman.

Chairman TOM DAVIS. Thank you.

Ms. Norton.

Ms. NORTON. Thank you very much, Mr. Chairman.

Thank you for your testimony, Mr. McHale. I'm also a member of the Aviation Subcommittee and, of course, have followed your work. As a result, I have followed your work very closely.

The recent transportation bill passed in the Congress took away from the TSA an issue that the chairman will be as interested in as I am involving this particular region, and that is that, of course, it's the capital of the United States, major business area, national capital, world capital, and you can't bring a charter plane here. You can bring it to New York where September 11 occurred. You can bring it to Dulles out of which the plane that landed at the Pentagon came. But you can't do it in D.C. I don't know what kind of message we were sending out, whether the message was we're scared, we're incompetent. But I have to give a great deal of credit to the chairmen of my committees, including the one you just heard from, because what we now have in that bill essentially takes it from the Transportation Security Administration, and I want to understand what your role will be, if any.

The bill says the Secretary of Homeland Security shall develop and implement a security plan to permit general aviation aircraft to land and take off at Ronald Reagan National Airport. It says the Administrator of the FAA shall allow general aviation aircraft that comply with the requirements, etc., of the security plan to land here. It even says that the President, if he suspends the security plan, has to give the reasons for it to Congress within 30 days.

I mean, this tells you a lot about how fed up we are with having general aviation taken from the capital of the United States. Now I'm not blaming the TSA for this. In fact, we believe that the FAA prepared a plan and that the security types essentially become the decisionmakers in matters like this. I would like to know, to what extent will the TSA be involved, particularly given the role you have had with commercial aviation?

Mr. MCHALE. That provision, I believe, is in the FAA reauthorization bill.

Ms. NORTON. It's the FAA reauthorization.

Mr. MCHALE. It's not quite passed yet but is, presumably, about to be passed in Congress, and we're certainly expecting it. We've worked with general aviation around the country to develop security programs.

Ms. NORTON. So you all have done it elsewhere and you are going to do it here.

Mr. MCHALE. We definitely have it elsewhere in the country, and we will work with them to establish an appropriate plan and move

that forward. I know you've had the intelligence briefings on the National Capital threat and——

Ms. NORTON. You know, if I may say so, just for the record, the intelligence briefings were—if this is the way we do intelligence in this country, then I tell you we all ought to get under our tables and not come up from a long time because, essentially, the intelligence briefing was your worst-case scenario. You know, if in fact the world—if in fact everything fails, if we are incompetent enough so that we don't know how to protect those things, then maybe some monument or maybe even the Capitol or some other such structure will be hit.

If anything, sitting in there was the chairman, from whom you just heard, after that briefing which occurred about a year ago, this is what you get. That's just how unconvincing dealing with security on a "the-sky-is-falling" basis will get you in a free society. What it means is you ought to close down not only commercial charter or general aviation, you'd better close down a lot more if that's the way we go about security.

Mr. MCHALE. Well, TSA has always taken its mission very seriously; and its mission is not to shut down aviation, not to shut down transportation——

Ms. NORTON. That's why we want you involved, because you have the only experience in this, Mr. McHale.

Mr. MCHALE [continuing]. But in fact it is to protect the freedom and movement of people and commerce. And that mission statement, I think, carries a lot of meaning and lot of balance.

Ms. NORTON. So you can assure me that, although we have taken this from the Transportation Department, that TSA will be involved.

Mr. MCHALE. We will continue to be involved, along with, obviously, providing advice to the Secretary as he proceeds.

Ms. NORTON. Mr. McHale, let me ask you to clarify very serious allegations that have been made. We simply want to know what the real deal is. It concerns the No-fly List. There have been now repeated allegations by anti-war activists that they are being targeted for scrutiny when they—because they have exercised their first amendment rights, that somebody has their names. Does the TSA have any records as a part of its No-fly List of individuals who have engaged in protests or criticize the government? Or do you have any way to find out who has engaged in protest activity in criticism of the government? Do you seek that information at all as a part of your work with the No-fly List?

Mr. MCHALE. Criticizing the government is not a basis to get on the No-fly List, and there is no one on the No-fly List as the basis of criticizing of the government.

Ms. NORTON. Or for engaging in demonstration of some kind?

Mr. MCHALE. What we look for is someone who has threatened civil aviations, has been a terrorist. And obviously—or has been—is associated with terrorists. Such—I mean, I want to be careful how I answer this because I—we do not put somebody on the list because they protested, but I don't want to say that someone who is associated with the terrorists may not have also protested. But you have to be associated with a terrorist or you have to be a ter-

rorist or a threat to civil aviation. Those are the kinds of things that we look for to put somebody on the No-fly List.

I've read the various newspaper allegations of these individuals. None of the activities that they cite are—provide any basis to put them on the No-fly List, and they would not be on a No-fly List on that basis.

Ms. NORTON. I appreciate that assurance.

One more question, if I might. I notice in your testimony on page 3 in speaking about the October 16 incident at Southwest Airlines, you found two types of prohibited items. One of them, besides the box cutters that everybody talks about, was liquid bleach secreted in a suntan lotion bottle. This leads me to ask you to be concerned about biological substances, chemical substances. Do we have any way to protect—are we even looking to protect against chemical substances, biological substances that could do harm on an airplane?

Mr. MCHALE. Let me say yes to that, but let me offer an off-the-record briefing on it, if I could, or a closed session briefing.

Ms. NORTON. I think we need one on that, particularly given this incident.

Chairman TOM DAVIS. OK. Thank you very much.

Mrs. Blackburn, you have a question I understand.

Mrs. BLACKBURN. Yes, thank you, Mr. Chairman; and thank you to our witness for your patience today as we are up and down and about. I do have a couple of questions for you, and I would like to really focus on some of the employee personnel situations with you.

I think one of the biggest complaints we get in our office is from people who go to one of the airports in our district where there are tremendously long lines. They are running late for a plane. There are TSA employees who are standing around and there are screening areas that are not open, and so they are left to stand and just steam. And the attitude of many of the employees is, I guess you would say almost disrespectful. They're not anxious to explain why there may be a delay or if there's a problem with equipment or equipment not working. So we hear a lot about that in our offices.

What I'd like to do is ask you how many total employees do you have right now?

Mr. MCHALE. We have approximately 40—between 47 and 48,000 screeners on board, and then we have about another 8,000——

Mrs. BLACKBURN. And qualifications required of those screeners? Do you have something you could send to my office that would list the qualifications necessary?

Mr. MCHALE. Yes, it's actually set out very specifically in the Aviation and Transportation Security Act, what they have to do.

Mrs. BLACKBURN. And education?

Mr. MCHALE. It includes at least a high school education or experience as a screener.

Mrs. BLACKBURN. But no experience necessary in any kind of law enforcement?

Mr. MCHALE. No, although there is a preference built into the statute for that kind of experience as well as military experience.

Mrs. BLACKBURN. And how heavily do you weight that preference?

Mr. MCHALE. I'm sorry?

Mrs. BLACKBURN. How heavily do you weight that preference?

Mr. MCHALE. It gives them I believe a—pushes them to the top of the line, but I don't actually know what the weighting is on that.

Mrs. BLACKBURN. OK. And then could you provide that answer to me, please?

Mr. MCHALE. Absolutely.

Mrs. BLACKBURN. Thank you.

OK. As you look at your recertification of these employees—let me back up a minute. When you train them, then you're putting them through 40 hours in the classroom and 60 hours on-the-job training before they're put behind the screen.

Mr. MCHALE. That's correct. About 44 hours in the classroom and 60 hours on the job.

Mrs. BLACKBURN. OK. Thank you.

And then your recertification, how much time will they spend going through this process and what is your expected cost each year of your recertification?

Mr. MCHALE. There are three parts of the recertification. There's a sort of a check on their current knowledge of the standard operating procedure. There is a review of their techniques in actually performing the screening, and then there is a multiple——

Mrs. BLACKBURN. OK. Just a minute. Did you just say 3 years?

Mr. MCHALE. Three parts, I said.

Mrs. BLACKBURN. Three parts.

Mr. MCHALE. Three parts. The first part is essentially a test of their knowledge of the standard operating procedure. The second is a review of their techniques and conducting an actual screening. The third is image mastery. They look at a computer and have to identify threat images on that. That basically requalifies them in all the skills they need to be a screener.

I do not know the annual cost of that. I can get that for you. The test is usually administered in those three parts separately so we do not disrupt the screening schedule that much. So that can actually take over a period of weeks to complete the recertification. We will have recertified every screener by March 1st next year, most of them well before that.

Mrs. BLACKBURN. OK. Thank you.

Now are you in the process of developing a separate system for airports that want to opt out of the Federalized program and go to a private program?

Mr. MCHALE. The testing and training procedure for the screeners will be the same. We are, however, looking toward November 19, 2004, to set up the process. We actually are doing a complete evaluation at this point. We've just hired BearingPoint as our contractor to help us evaluate the contract screeners versus the Federal screeners and the contracting system versus the Federal system. So that process works through——

Mrs. BLACKBURN. Is BearingPoint going to develop your benchmarks on that or will GAO do that for you?

Mr. MCHALE. BearingPoint will do that.

Mrs. BLACKBURN. BearingPoint will do that?

Mr. MCHALE. I think GAO is doing a related study, and we'll certainly take that into account.

Mrs. BLACKBURN. Excellent. Thank you.

Thank you, Mr. Chairman.

Chairman TOM DAVIS. Thank you very much.

Let me just ask a couple of questions, Mr. McHale. In your testimony you talked about a sword that was hidden in a cane, a gun that was found in a teddy bear and a knife that was discovered in a sealed soda can. The circumstances surrounding these instances—if somebody puts a knife in a soda can, they couldn't be up to any good.

Mrs. BLACKBURN. I would not think so.

Chairman TOM DAVIS. A gun in a teddy bear. I mean, what were the circumstances around that? Have we actually caught terrorists as a result of this, or are these just bumbling people who like to carry guns in teddy bears?

Mr. MCHALE. Well, there's a lot of people who believe that they need to carry protection for various reasons and a lot of reasons why people might try to carry a knife and a gun with them other than terrorism. I don't think it would be fair to say that we have actually found an item that we've associated directly with a terrorist at this point. The gun in the teddy bear is still a very strange incident and has been under investigation. The limited amount I can say about it is that it appears that the teddy bear was given to the child at a hotel by someone the child did not know and then the child carried it to the checkpoint and the gun was found in the teddy bear. A very bizarre, truly bizarre incident. The sword cane was a sword cane, and the person was carrying the sword cane, and they've been referred for prosecution. And I believe that's the same case with the knife in the soda can.

Chairman TOM DAVIS. But the gun in the teddy bear, as far as you know, somebody gave to a kid?

Mr. MCHALE. That's correct.

Chairman TOM DAVIS. Did we find out who gave it to him?

Mr. MCHALE. I don't believe they've done that yet. That's still under active investigation.

Chairman TOM DAVIS. OK. We're going to hear testimony in the second panel from private screening companies that participated in the program that they're having problems implementing screening procedures that are more stringent than the current TSA practices. That's what they're going to testify to. Can you give me your understanding of the TSA's position on the flexibilities given to the private pilot program airports in conducting the screening?

Mr. MCHALE. The screening standard operating procedure for the private pilot airports and for the TSA airports is identical. They use exactly the same SOP.

Chairman TOM DAVIS. What if they want to be tougher, if they have something that's going to be a little more stringent protocol? Are they barred from doing that?

Mr. MCHALE. They would be barred from doing that, or at least they'd have to bring it to us and we'd have to review it. Again, we always have to strike a balance here. You know, you can have security at a level at which you'd completely deter people from traveling. We need to strike the right balance. So our standard operating procedure is designed to do that.

Chairman TOM DAVIS. You know, as I've traveled around the country and talked to some of these screeners, some of them had pretty good jobs and they really feel like they're on the war against terror. They want to contribute, and they saw what happened on September 11, and they want to be a part. I mean, it's different in different areas, I guess. My impression is it's been pretty good people for the most part, and it's our job then to make sure that they're appropriately trained but you're dealing with a good quality of people.

We have a huge travel rush coming up next week in this country——

Mr. MCHALE. Right.

Chairman TOM DAVIS [continuing]. And it's very difficult when you try to look at your priority, which is protecting the airlines, making sure they're going to be safe and people who are in a holiday rush with all of the other pressures that holidays put on individuals and families and so on. Have you talked to your people down the line? What are we doing to try to make this week—do we have extra people coming in for shifts?

Mr. MCHALE. What we're doing, we have a mobile screening force we use to deal with problems at particular airports that we keep ready at all times to dispatch, and they'll obviously be fully dispatched over the Thanksgiving holidays to the pressure points in the system.

In addition, we still have some airports that probably have an excess of staff compared to other airports. We are identifying those within each of the five areas that we divide the country up in to and we will reassign that staff. Obviously, there'll be overtime; obviously, there'll be some leave restrictions over that period. We have to constantly look at how we treat our screeners. As you said, they are very good. They are very dedicated people. We want to hold on to them.

We had some real rough times the first year that we got them up. We didn't have the infrastructure in place to support them. We've corrected a lot of those problems now. I think we are treating them better than they were treated in the past, and we're trying to set up a lot of systems to listen to them. Because they do have good ideas and they have very good ideas about how to improve their jobs. So we're working with them to do that.

For the holiday rush, obviously a lot of what we have to do is educate people that there will be longer lines, educate people as they approach the checkpoint to prepare and help our screeners deal with the pressure because the worst thing that can happen is for the lines to get longer, the passengers to get upset, put more pressure on the screeners and cause some security lapses. So we need to keep on working on that and make sure our screeners understand that we will support them as they do their job and that their No. 1 job is to keep threat objects off——

Chairman TOM DAVIS. Again, if somebody's in the back of the line and running late, do you have a way to try to get them up to the front?

Mr. MCHALE. We work with the airlines on that. The airlines usually try to take care of that; and if they'll bring somebody up, we'll try to handle it.

Chairman TOM DAVIS. Great. Well, thank you very much for being with us.

I'm going to hand the gavel over to Mr. Shays for a little bit. I've got to run to another meeting but I will be back. Thank you very much.

Mr. MCHALE. Thank you, Mr. Chairman.

Mr. SHAYS [presiding]. Thank you, Mr. McHale, for being here. I think you and the chief administrator have one of the most difficult and unwanted jobs you could have. I say this for the simple fact that you could wake up tomorrow and six planes could be blown out of the sky and you will be blamed for it even though you don't yet have the capability to prevent it. That's the reality. I know you can't tell people that can happen, but that's the reality. But I can, as a Member of Congress, say that we know; and when I fly, I know a plane can be blown out of the sky.

I want to ask you—I do have a basic question that says, you know, how safe are we to fly? And I think your answer—basically someone else's—is we're a lot safer than we were. We're a lot safer, and we continue to be safer each and every day. But we don't feel as safe because we had a false sense of safety before September 11. Do you disagree with anything I have said?

Mr. MCHALE. I agree completely with what you said.

Mr. SHAYS. Thank you. Let me ask you, when I look at—and we're going to have—I want to just nail down a little better what the attitude is of TSA as it relates to private security. Are they being given the capability to prove their worth if, in fact, you're the ones that are training them?

Mr. MCHALE. I think the answer to that is yes. The statute is pretty prescriptive requiring them, for example, to have the same training, the same qualifications, the same pay and benefits, or similar—equivalent, I believe, is the word—equivalent pay and benefits. So the statute puts a lot of fairly tight restrictions around what they can do.

Obviously, when we set out to do this in 1 year, meet the deadline both with the Federal screeners and the private screeners, we didn't have a lot of opportunity to make five separate little plans for the private screeners. So what we set out to do was, we trained them all with our training contract to the same standard. That way we know that on November 19 last year and on December 31 last year, we had at every airport in the country people who had gone through the same training regime.

We are talking to the various contractors about proposals that they may have to give them more flexibility within this framework we have in the statute, but that could include things such as taking on some of the training responsibilities and that sort of thing. Obviously, we'd need to monitor that very closely. But those are the kind of things we could look at.

Mr. SHAYS. But do they have the resources to provide greater training if they choose to?

Mr. MCHALE. We'd have to modify their contract because, right now, their contract doesn't reimburse them for that. So that would have to be negotiated within the contract. Presumably some of them have resources and some of them don't, but that's something that would have to involve a contract modification.

Mr. SHAYS. So to have greater training they'd have to just do it out of their own pocket?

Mr. MCHALE. At this point, yes.

Mr. SHAYS. OK. As it relates to the issue, I think we've covered a little bit the weapons brought on the plane by the young student. I want to talk about the young man who put himself in a box and basically sent himself from New York to Dallas. Would there have been anything under our present system to have prevented him from being wrapped in a bomb and our being able to detect him? He still would have been in that box, correct?

Mr. MCHALE. That's correct. There would have been—that's correct.

Mr. SHAYS. He still, potentially, could have had some firearms on him?

Mr. MCHALE. Yes.

Mr. SHAYS. So, I mean, it was a real breakdown. But the breakdown was he was cargo, correct?

Mr. MCHALE. That's correct. He was on an all-cargo carrier.

Mr. SHAYS. Why should I feel any comfort—and that happened to be by—in a sense, he could have possibly been put on a passenger plane, correct? I mean, cargo is put on passenger planes.

Mr. MCHALE. Cargo is. We do have more restrictions on cargo that can go on all passenger aircraft, including things like the "known shipper" program and other things.

Mr. SHAYS. Well, I'm not going to jump up and down with the "known shipper" program.

Mr. MCHALE. Right.

Mr. SHAYS. "Known shipper" is not screening. We call it that, but it's not screening. It is just knowing the shipper. We don't screen the packages of known shippers.

Mr. MCHALE. We do not do explosive-grade detection screening on it; that's correct.

Mr. SHAYS. Do we do other kinds of screening?

Mr. MCHALE. Well, the statute does define, as you've noted, that a known shipper is a screening program.

Mr. SHAYS. And so—but you and I aren't going to play that charade.

Mr. MCHALE. Right.

Mr. SHAYS. Knowing who the shipper is does not mean you screen the package.

Mr. MCHALE. I think most people, when we say screening, think of some sort of physical screening of the package or x-ray screening of the package. We do not do that.

Mr. SHAYS. Well, what do you think of it as?

Mr. MCHALE. By law, it's screening; and that is what we have available to us given the type of technology that we have in the operational environment. We have to continue to improve that technology. We need to continue to work on it. But the "known shipper" program is a tool like a lot of our other tools.

Mr. SHAYS. I'm going to say it's a tool. But I want to really not have the record be unclear here. The law says we can call it screening when we know who the shipper is. Is any of the cargo screened by knowing who the shipper is? And the answer is no.

Mr. MCHALE. By law, yes. That's—and obviously——

Mr. SHAYS. I'll use another word then.

Mr. MCHALE. OK.

Mr. SHAYS. By law, it is only because Congress made it that way. Because it's like Congress passing a law that says that it's sunny every day.

Mr. MCHALE. Right.

Mr. SHAYS. If we passed a law saying it's sunny every day that doesn't mean it's sunny every day just because we passed a law saying that, and it's about as absurd as saying that, and I know why Congress did that and I think you doo too. But it is misleading to the public because it implies that their luggage is being screened. I'll tell you why I think the public is being misled. I was misled because I thought we screened all packages because I saw the word screening; and I learned, frankly, from my colleague from Massachusetts, that we don't.

Mr. MCHALE. I think we have tried to be very clear, and we have been certainly in recent months as we've turned heavily to the air cargo area as we've developed our air cargo strategy to make it clear what the "known shipper" program is and is not and that it is not physical and technological screening. We stressed that we need to do that screening.

Of course, the program we've announced this week will require random physical or x-ray screening of the cargo on both passenger and all cargo aircraft. The specific——

Mr. SHAYS. When?

Mr. MCHALE. We issued the directive this week.

Mr. SHAYS. That it will be done when?

Mr. MCHALE. I believe it's effective within 72 hours of the issuance, so it's probably effective about now.

Mr. SHAYS. Are you saying all cargo is being screened physically?

Mr. MCHALE. A random screening of the cargo.

Mr. SHAYS. So it's random, but it's not—and random is 1 percent, 2 percent?

Mr. MCHALE. That's in the security directive, which is sensitive security information. I'll be happy to provide that to you in closed session.

Mr. SHAYS. The bottom line is we do not physically screen all packages that——

Mr. MCHALE. We do not physically screen all packages.

Mr. SHAYS. And so it is very possible that weapons, it is very possible that explosives can be put on a passenger plane via cargo that is placed in the passenger plane; is that not correct?

Mr. MCHALE. I think the—I think I probably have a little more faith in the "known shipper" program.

Mr. SHAYS. I didn't ask you about your faith.

Mr. MCHALE. That——

Mr. SHAYS. Mr. McHale, I don't care about your faith. I care about reality. The reality is, it can be done; correct or not correct?

Mr. MCHALE. There is no system of security that cannot be evaded.

Mr. SHAYS. That's not what I asked. That's not what I asked.

Mr. MCHALE. Well, then, Mr. Shays, the answer to that question obviously is yes.

Mr. SHAYS. No.

Mr. MCHALE. The answer is yes.

Mr. SHAYS. No, but the—because—we both agree that you can break through any system.

Mr. MCHALE. Right.

Mr. SHAYS. But at least when we check the baggage in an aircraft we are checking every bag, correct?

Mr. MCHALE. That's correct.

Mr. SHAYS. Physically.

Mr. MCHALE. That's correct.

Mr. SHAYS. And so we make it a lot more difficult. If in fact we are not checking what is cargo on an airplane that could be on a passenger plane, if in fact that cargo, instead of being on a cargo plane is put on a passenger plane, it is physically unscreened, correct?

Mr. MCHALE. Unless it's subject to the random screening, that is correct.

Mr. SHAYS. Right. How do you feel about that?

Mr. MCHALE. I'm told, actually the security directive is effective in a little over a month. We've given them a month to put it into effect.

Mr. SHAYS. I just want to know how you feel about the fact that we don't physically screen——

Mr. MCHALE. I would like to have screening of every item that goes on an aircraft. The fact is the systems are simply not in place at this time. For us to require that we would have to shut down large portions of the air cargo system. It's our job to try to come up with a way to keep things moving as well as secure. We don't want to hand the terrorists an unearned victory.

Do I feel comfortable about it? No. I think we need to keep on tackling the issue, keep on working the issue as hard as we can, come up with the best ways we can to secure the cargo and aircraft, but I don't think it would be appropriate at this time to bar cargo from aircraft.

Mr. SHAYS. Why don't we do what we did when we did the checking for baggage? I know this part of it because I refused to vote for the TSA bill in November unless we had a deadline for screening. We put the deadline for screening, the end of 2003, but in order to get my vote, they did that. And it passed by what, how many votes?

Mr. MCHALE. I think it passed quite handily at the end of the day, did it not?

Mr. SHAYS. OK. It was a close vote.

Mr. MCHALE. Oh, I'm sorry.

Mr. SHAYS. It was a close vote.

But let me ask you this. When it got out of the House, that's what it was. My point, though, is we were told it couldn't physically be done by the end of 2003. Then when it came back from conference, it said the end of 2002. So I go to my leadership and I say, well, if we couldn't do it by 2003, how could we do it by the end of 2002? And the response I got was that they did not want there to be more than 12 months or 14 months in which we were saying to the American people we weren't going to physically screen all baggage. Well, ultimately, when did we—do we physically screen all baggage today?

Mr. MCHALE. Yes, we do.

Mr. SHAYS. And when did we meet that deadline?

Mr. MCHALE. December 31, 2002.

Mr. SHAYS. Right. Why shouldn't we put the same deadline on cargo?

Mr. MCHALE. The difference is this: We obviously went to extraordinary lengths to meet that deadline, and we did, and I'm very proud of that. The technology was in place and in use in airports to detect explosives in baggage. Very little of it, but it was there. In 2000, 40 machines had been ordered worldwide. We had to basically redesign the production systems, which we did and we could do, to bring that total up to 1,100 bought and installed in 2002 to meet the deadline, plus 5,000 of the trace detection machines.

Cargo comes in all sorts of different shapes and sizes for aircraft and it comes in all different varieties. It's a very—it's a much more difficult problem to do explosive detection on cargo than it is on baggage, and we do not have the machines in place to do that. We do have machines that can x-ray cargo but that doesn't detect.

Mr. SHAYS. What you just said, though, is something known by the terrorists, so you didn't disclose anything.

Mr. MCHALE. I did not disclose anything to them.

Mr. SHAYS. Right. Then why wouldn't we—and we'll get on here—but why didn't we—or why wouldn't you recommend or why wouldn't you set your own deadline for saying that all cargo on a passenger plane will be checked by a certain deadline?

Mr. MCHALE. We have an aggressive R&D program. Congress has given us quite a lot of money for that this year. I believe it's close to $150 million for the R&D program. And we also have additional funds in the Department of Homeland Security budget in the Science and Technology Directorate. We're going to aggressively pursue that technology. Once we have the technology, once we have the systems, then I think a deadline is appropriate to drive them into the operational side of the system. But if we don't have the technology, it's kind of—a deadline makes it—you know, I'm not confident as to the—I could not today tell you when we'll have the technology that's available. We're trying to do it.

Mr. SHAYS. The problem is that we have an example of a deadline that nobody wanted that we ended up having that we met.

Mr. MCHALE. Right.

Mr. SHAYS. And I'm struck by the fact that what goes in the belly of an aircraft that's a passenger plane is probably not going to be as large as containers for cargo.

Mr. MCHALE. That's true. We do have a couple of programs that we're doing. One is, for example, we are using canines to detect potential explosives in mail that go in the passenger planes. We've also got canines out there working with us on inspecting some of the cargo in passenger planes, the smaller packages. You know, dogs are pretty useful for a lot of things but there are some types of cargo, especially palletized cargo, where they're not all that helpful. But we're trying to bring them online as well as the technology solution. We know dogs work, so—and that's the technology that's there. They take, obviously, a long time to deploy. But that's something that we're working on, too.

Mr. SHAYS. Do we know when we have that it's going to go on a passenger plane versus a cargo plane? Does TSA have a sense of that?

Mr. MCHALE. We know that there's only certain cargo that can go on passenger planes and we know what that is. But cargo that can go on a passenger plane could also go onto an all-cargo plane.

Mr. SHAYS. Right. Let me just—before getting to our next panel, give me a sense of why I should feel comfortable about the screening, the effort we do to protect our aircraft from employees who work at the airport? I'm told, but it's basically more rumor than fact so I'll say that to you, that we don't do a particularly good job of checking who gets on the airplane, workers who get on, that they have much freer access to the field and that we leave ourselves vulnerable. Do you think that's a concern?

Mr. MCHALE. I don't think it's as much of a concern as perhaps has been suggested. We do have basically three types of employee: employees who have access to the secure area, which is generally the ramp, unescorted access on the secure area, which is basically the ramp on which the aircraft are parked and the aircraft; employees that have access to the sterile area, which is the area beyond the checkpoint; and then employees who have regular escorted access to aircraft or other secure areas of the airport. All of those employees are subjected to a background investigation which includes a check of the terrorist data bases and intelligence data bases as well as the criminal history records, and we update that periodically. We have conducted over—we have updated all of them since September 11. We've conducted well over a million background checks in that area to understand that very—and quite a few people have been removed as a result of those background checks.

Mr. SHAYS. All right. Is there anything that you would like to put on the record before we get to the next panel?

Mr. MCHALE. The only last thing, just on the air cargo, just to note that we have been working very carefully with the Aviation Security Advisory Committee. It's a committee that consists not only of industry members but also consumer groups, passenger groups, the victims of Pan Am 103, and other groups. We have worked with them to develop a strategic plan. As I mentioned, the security directives that we issued this week are in fact beginning to implement the strategic plan, air cargo strategic plan that we announced early this week.

Mr. SHAYS. Mr. McHale, let me just thank you for I know what is a 7-day-a-week job, probably 24 hours a day; and I have a feeling you don't sleep as well as some of us sleep.

Mr. MCHALE. I think that's correct.

Mr. SHAYS. And we thank you for your service to your country.

Mr. MCHALE. Thank you very much.

Mr. SHAYS. Thank you.

Our second panel is Cathleen Berrick, GAO Director of Homeland Security and Justice Issues; John DeMell, president of FirstLine Transportation Security; and James McNeil, president of McNeil Security, who is accompanied by Mike Broida, site manager, Greater Rochester International Airport.

Anyone else who may be accompanying them who might be called to respond to questions, we'd like you to stand as well and we'll swear you in. Is there anyone that might be accompanying you that you might ask to respond to a question? If so, they can stand up and be sworn, and then if you're not—if you don't end up speaking it would—it saves us the trouble of swearing you in again. Is there anyone else? Are we all set?

[Witnesses sworn.]

Mr. SHAYS. Note for our record that our witnesses have responded in the affirmative.

Ms. Berrick, we'll have you go and then Mr. DeMell and then Mr. McNeil. We'll have you give your testimony, and then we'll ask you questions.

Ms. BERRICK. Thank you.

Mr. SHAYS. Can you just suspend 1 second, please?

Ms. BERRICK. Sure.

Mr. SHAYS. Thank you. I'm sorry to interrupt. We'll start all over.

Let me just tell you I'm going to give you 5, and then I'll roll over, but I'd like you to finish in a minute or two after that. So it'll be 5 minutes.

Ms. BERRICK. OK. Certainly.

Mr. SHAYS. With a little bit of leeway.

STATEMENTS OF CATHLEEN A. BERRICK, DIRECTOR, HOMELAND SECURITY AND JUSTICE ISSUES, GENERAL ACCOUNTING OFFICE; JOHN DEMELL, PRESIDENT, FIRSTLINE TRANSPORTATION SECURITY; AND JAMES MCNEIL, CHIEF EXECUTIVE OFFICER, MCNEIL TECHNOLOGIES, INC., ACCOMPANIED BY MIKE BROIDA, SITE MANAGER, GREATER ROCHESTER INTERNATIONAL AIRPORT

Ms. BERRICK. Thank you. Thanks again for the opportunity to participate in today's hearing on the security of commercial aviation and, in particular, passenger screening.

Since the attacks of September 11, numerous changes have been made to strengthen passenger screening, including the Federalization of screeners and the enhancement of screening operations. However, recent reviews and testing conducted by GAO and others and recent media reports have revealed continuing vulnerabilities in screening. My testimony today focuses on three areas that we believe are fundamental in strengthening passenger screening. These areas include measuring the effectiveness of the current screening operation through increased testing and collection of performance data; second, strengthening screener training; and, third, assessing the performance of pilot airports using contract screeners and preparing for the potential transition of other airports to private screening companies. These conclusions are based on our preliminary assessment of TSA's passenger screening program. We have an ongoing review assessing these areas in further detail.

We found that TSA has collected limited information on the effectiveness of passenger screening but is taking steps to collect additional information. For example, TSA's primary source of information on the effectiveness of its screening program is through covert testing conducted at security checkpoints. However, we found that,

as of August 2003, TSA had only tested about 2 percent of its screening work force.

Another key source of screener performance data is the Threat Image Projection system [TIP], which was deactivated after September 11 and hasn't been fully redeployed. TIP places images of threat objects on an x-ray screen during actual operations to record whether screeners detect a threat object.

We also have found that TSA has not fully deployed an annual recertification program for screeners that would provide additional performance data. As I mentioned, TSA is taking actions to begin collecting additional performance data, including doubling its covert testing. Fully reactivating TIP by the summer of 2004 is what they have planned as well as establishing a screener certification program.

We also found that TSA should strengthen its recurrent and supervisory training programs. TSA cited a lack of training and effective supervision as primary causes for screening testing failures during the covert tests. However, TSA has not fully developed or deployed these programs. Recurring training is the ongoing training of screeners on a frequent basis to enhance their skills and introduce them to additional threat objects.

Some screening supervisors we interviewed also reported that they had not received any specialized training to assist them in their supervisory role. TSA is taking positive steps in this area, including deploying some recurrent training modules and tailoring an off-the-shelf supervisory course to meet the needs of its training supervisors. However, we feel that they could do more in this area. Finally, TSA wants to determine how to evaluate the performance of the five pilot airports that are using private screeners and prepare for airports potentially opting out of using Federal screeners beginning in November 2004.

Both of these efforts will be challenging for the following reasons: First, TSA recently issued a contract to begin assessing the performance contract pilot airports. However, since TSA has collected limited performance data on screening operations, it will be difficult for the contractor to assess how well the pilot airports have been performing. Second, since the pilot airports have been granted only limited flexibilities in running screening operations, this could limit TSA's ability to effectively assess whether efficiencies could be achieved by using private screening conditions. Third, TSA has not yet established a process to evaluate airports that may apply to opt out of using Federal screeners or determine the impact that this may have on TSA's staffing and oversight requirements.

We are encouraged that TSA is taking steps to strengthen its passenger screening program and believe that they should continue to focus in on the areas of performance, management, training, and contract screening. We will continue to review TSA's efforts in these areas as we conduct our analysis of the passenger screening program.

Mr. Chairman, this concludes my opening statement. I'd be happy to respond to any questions at the appropriate time.

Mr. SHAYS. Thank you. Did you take a breath during that entire time?

Ms. BERRICK. I wanted to get it in within 5 minute.

Mr. SHAYS. I know. But I didn't want you to feel you had to. Thank you for your testimony.

Ms. BERRICK. Thank you.

[The prepared statement of Ms. Berrick follows:]

United States General Accounting Office

GAO

Testimony
Before the Committee on Government Reform, House of Representatives

For Release on Delivery
Expected at 10:00 a.m. EST
Thursday, November 20, 2003

AVIATION SECURITY

Efforts to Measure Effectiveness and Strengthen Security Programs

Statement of Cathleen A. Berrick, Director,
Homeland Security and Justice

GAO-04-285T

November 2003

GAO
Accountability·Integrity·Reliability
Highlights

Highlights of GAO-04-285T, a report to the Committee on Government Reform, House of Representatives

AVIATION SECURITY

Efforts to Measure Effectiveness and Strengthen Security Programs

Why GAO Did This Study

Commercial aviation has been a long-standing target for terrorists. Since the tragic attacts of September 11, 2001, substantial changes have been made to enhance security—including the creation of the Transportation Security Administration (TSA) and the federalization of the passenger screener workforce. However, despite these changes, vulnerabilities in aviation security continue to exist. Accordingly, GAO was asked to describe TSA's efforts to (1) measure the effectiveness of its aviation security initiatives, (2) strengthen its passenger screening program, and (3) address additional challenges in further enhancing aviation security.

What GAO Recommends

In prior reports and testimonies, GAO has made numerous recommendations to strengthen aviation security. We also have ongoing reviews assessing many of the issues addressed in this testimony and will issue separate reports on these areas at a later date.

www.gao.gov/cgi-bin/getrpt?GAO-04-285T.

To view the full product, including the scope and methodology, click on the link above. For more information, contact Cathleen A. Berrick at (202) 512-8777 or Berrickc@gao.gov.

What GAO Found

TSA has implemented numerous initiatives designed to enhance aviation security, but has collected limited information on the effectiveness of these initiatives in protecting commercial aircraft. Our recent work on passenger screening found that little testing or other data exist that measures the performance of screeners in detecting threat objects. However, TSA is taking steps to collect additional data, including developing a 5-year performance plan detailing numerous performance measures, as well as fielding the Threat Image Projection system and increasing screener testing.

In addition to collecting performance data, TSA could further strengthen passenger screening by fully deploying recurrent and supervisory training programs, determining the appropriate levels of screeners at the nation's airports, and improving oversight of the contract screener pilot program. Although TSA has developed and deployed basic and remedial training programs, it has not fully developed or deployed recurrent or supervisory training programs. In addition, TSA acknowledged that its initial staffing efforts created imbalances at the nation's airports, and that it has taken limited action to assess the performance of the pilot airports using private, versus federal, screeners. TSA is undertaking a number of actions to address these concerns, including strengthening its training program and awarding contracts to assess its staffing model and the performance of the contract pilot airports.

TSA faces a number of other challenges as it continues to enhance aviation security. Significant challenges include implementing the Computer-Assisted Passenger Prescreening System (CAPPS II), as well as strengthening baggage screening, airport perimeter and access controls, and air cargo and general aviation security. In implementing CAPPS II, TSA must ensure it addresses concerns surrounding travelers' privacy rights, the accuracy of databases used by CAPPS II, and obtaining international cooperation needed for the system to be fully operational. Additional challenges include integrating explosive detection systems into airport's in-line baggage handling systems, identifying cost-effective perimeter security technologies, effectively targeting air cargo for screening, and improving security at general aviation airports. Further, TSA faces challenges in funding increased aviation security measures and ensuring that these costs are controlled.

Security Screeners Checking Passengers with a Hand-Held Metal Detector

Source: FAA.

Mr. Chairman and Members of the Committee:

Thank you for inviting me to participate in today's hearing to discuss our recent work on the Transportation Security Administration's (TSA) efforts to assess its performance and strengthen its security programs, to include passenger screening. Securing commercial aviation is a daunting task—with hundreds of airports, thousands of aircraft, and tens of thousands of flights daily carrying millions of passengers and pieces of baggage and cargo. Since the attacks of September 11, 2001, billions of dollars have been spent, and a wide variety of programs and initiatives have been implemented to enhance aviation security. However, recent reviews and covert testing conducted by GAO and the Department of Homeland Security's Office of Inspector General, as well as recent media reports, indicate that weaknesses and vulnerabilities in commercial aviation continue to exist. For example, the incident involving a college student who placed box cutters, clay resembling plastic explosives, and bleach on commercial aircraft show that aviation security can still be compromised.

My testimony today highlights three key areas that TSA must focus on to enhance aviation security. These areas include (1) measuring the effectiveness of TSA's aviation security initiatives that have already been implemented, (2) strengthening its passenger screening program, and (3) addressing key programmatic and management challenges to further enhance aviation security. My testimony is based on our prior work, reviews of TSA documentation, and interviews with TSA officials.

In summary:

Although TSA has implemented numerous programs and initiatives to enhance aviation security, it has collected limited information on the effectiveness of these programs and initiatives. Our recent work on TSA's passenger screening program showed that although TSA has made enhancements in passenger screening, it has collected limited data on screeners' ability to detect threat objects. The Aviation and Transportation Security Act (ATSA), which was established with the primary goal of strengthening aviation security, requires that TSA establish acceptable levels of performance for security initiatives and develop annual performance plans and reports to measure and document the effectiveness

of those initiatives.[1] Although TSA has developed an annual performance plan and report as required by ATSA, to date these tools have focused on TSA's progress in meeting deadlines to implement programs and initiatives mandated by ATSA rather than on the effectiveness of these programs and initiatives. TSA has recognized that it has collected limited performance data on its security initiatives, and is taking steps to collect additional data, including developing a 5-year performance plan, and increasing passenger screener testing.

Our recent work on TSA's passenger screening program showed that the program can be strengthened in the areas of training, staffing, and the contract screener pilot program.[2] Although TSA has developed and deployed basic and remedial training programs, it has not fully developed or deployed recurrent or supervisory training programs to ensure that screeners are effectively trained and supervised. In addition, TSA has acknowledged that its initial screener staffing levels created imbalances at the nation's airports—a situation that it is attempting to address. TSA also has not yet determined how to evaluate and measure the performance of its contract screening pilot program. Since we issued our preliminary report on TSA's passenger screening program in September 2003, TSA has taken a number of actions to address these concerns, including enhancing its recurrent and supervisory training programs, and awarding a contract to assess the contract screening pilot program. However, TSA has recognized that assessing the performance of the pilot airports will be difficult because of a lack of performance data.

TSA faces a number of other challenges as it continues to address threats to our nation's aviation system. Significant challenges include implementing various aviation security programs, such as the Computer-Assisted Passenger Prescreening System[3] (CAPPS II), and addressing broader security concerns related to the security of air cargo and general aviation.[4] TSA also faces challenges in managing the costs of aviation

[1]P.L. 107-71.

[2]ATSA required TSA to implement a pilot program using contract screeners at five commercial airports. The purpose of the 2-year pilot program is to determine the feasibility of using private screening companies rather than federal screeners.

[3]CAPPS II is a system intended to perform a risk assessment of all airline passengers to identify those requiring additional security attention.

[4]General aviation consists of all civil aircraft and excludes commercial and military aircraft.

security and in strategically managing its workforce of about 60,000 people, most of whom are deployed at airports to detect weapons and explosives. TSA has been addressing these and other challenges through a variety of efforts. We have work in progress that is examining TSA's efforts in addressing many of these challenges.

Background

The security of the U.S. commercial aviation system has been a long-standing concern. As demonstrated by the 1988 bombing of a U.S. airliner over Lockerbie, Scotland, and the 1995 plot to blow up 12 U.S. aircraft in the Pacific region discovered by Philippine authorities, U.S. commercial aircraft have long been a target for terrorist attacks. Over the years, numerous initiatives have been undertaken to improve aviation security. However, as we and others have documented in numerous reports and studies, weaknesses continue to exist. It was because of these weaknesses that terrorists were able to hijack four commercial aircraft on September 11, 2001, with tragic results.

In an effort to strengthen the security of commercial aviation, the President signed into law the Aviation and Transportation Security Act (ATSA) on November 19, 2001. ATSA created TSA as an agency within the Department of Transportation with the responsibility for securing all modes of transportation, including aviation. ATSA mandated specific improvements to aviation security and established deadlines for completing many of these initiatives. Consequently, TSA's main focus during its first year of operation was on meeting these deadlines, particularly federalizing the screener workforce at commercial airports nationwide by November 19, 2002, while at the same time establishing a new federal organization from the ground up. On March 1, 2003, pursuant to the Homeland Security Act, TSA was transferred from the Department of Transportation to the new Department of Homeland Security.[5]

Virtually all aviation security responsibilities now reside with TSA. One of the most substantial of these is passenger screening. Passenger screening involves the use of metal detectors, X-ray machines, explosive trace detection machines, and physical searches to examine passengers and their baggage to identify threat objects. Passenger screening has historically been an area of concern. As we reported in 1987, and again in 2000, passenger screeners who conducted these examinations have had

[5]P.L. 107-296.

difficultly in detecting weapons and other dangerous objects. At the time we issued these reports, air carriers were responsible for performing passenger screening. With the passage of ATSA, this responsibility has now become the responsibility of TSA. TSA is also responsible for ensuring the security of air cargo, limiting access to restricted areas of airports to authorized personnel, securing airport perimeters, and conducting background checks for airport personnel, among other responsibilities.

Limited Information Exists on the Effectiveness of Aviation Security Initiatives

TSA has implemented numerous initiatives designed to enhance aviation security, but it has collected limited information on the effectiveness of these initiatives, particularly its passenger screening program. ATSA requires that TSA establish acceptable levels of performance and develop annual performance plans and reports to measure and document the effectiveness of its security initiatives.[6] Although TSA has developed these performance tools as required by ATSA, the tools currently focus on TSA's progress toward meeting ATSA deadlines, rather than on the effectiveness of its programs and initiatives. Although TSA has collected limited data on the effectiveness of its initiatives, it is taking several steps to collect objective data to assess its performance.

Evaluation of Program Effectiveness

Although there are a number of methods that TSA can use to measure the effectiveness of its passenger screening program, none are being fully utilized. As we reported in September 2003,[7] the primary source of information collected on screeners' ability to detect threat objects is covert testing conducted by TSA's Office of Internal Affairs and Program Review. However, TSA does not consider the results of these covert tests as a measure of performance, but rather a "snapshot" of a screener's ability to detect threat objects at a particular point in time and as a system-

[6]An annual performance plan is to provide the direct linkage between the strategic goals outlined in the agency's strategic plan and the day-to-day activities of managers and staff. Additionally, annual performance plans are to include performance goals for an agency's program activities as listed in the budget, a summary of the necessary resources that will be used to measure performance, and a discussion of how the performance information will be verified. An annual performance report is to review and discuss an agency's performance compared with the performance goals it established in its annual performance plan.

[7]U.S. General Accounting Office, *Airport Passenger Screening: Preliminary Observations on Progress Made and Challenges Remaining*, GAO-03-1173 (Washington, D.C.: Sept. 24, 2003).

wide performance indicator. At the time we issued our report, the Office of Internal Affairs and Program Review had conducted 733 covert tests of passenger screeners at 92 airports. As a result, only a small percentage of TSA's passenger screeners had been subject to a covert test.

In addition to conducting covert tests at screening checkpoints, TSA conducts tests to determine whether the current Computer-Assisted Passenger Screening System is working as designed; threat objects are detected during the screening of checked baggage; and access to restricted areas of the airport is limited only to authorized personnel.[8] While the Office of Internal Affairs and Program Review has conducted about 2,000 access tests, it has conducted only 168 Computer-Assisted Passenger Screening System and checked baggage tests. Based on an anticipated increase in staff from about 100 in fiscal year 2003 to 200 in fiscal year 2004, the Office of Internal Affairs and Program Review plans to conduct twice as many covert tests next year.[9]

Another key source of data on screener performance in detecting threat objects is the Threat Image Projection (TIP) system, which places images of threat objects on the X-ray screen during actual operations and records whether screeners identify the threat object.[10] The Federal Aviation Administration began deploying TIP in late 1999 to continually measure screener performance and to train screeners in becoming more adept at detecting hard-to-spot threat objects. However, TIP was shut down immediately following the September 11 terrorist attacks because of concerns that it would result in screening delays and panic, as screeners might have thought that they were actually viewing a threat object. Although TSA officials recognized that TIP is a key tool in measuring,

[8]The original Computer Assisted Passenger Screening System is a stand-alone application residing in an air carrier's reservation system that analyzes certain behavioral patterns to score and calculate each passenger's need for additional screening.

[9]Currently, the Office of Internal Affairs and Program Review has 7 team leaders assigned full-time to covert testing, and plans to have a total of 14 full-time team leaders by the end of fiscal year 2004. The team leaders draw from the remaining staff within the office, such as auditors and analysts, to perform the testing. According to TSA officials, overall, 95 percent of the staff in the Office of Internal Affairs and Program Review participates in covert testing as a collateral responsibility.

[10]TIP is designed to test screeners' detection capabilities by projecting threat images, including guns and explosives, into bags as they are screened. Screeners are responsible for positively identifying the threat image and calling for the bag to be searched. Once prompted, TIP identifies to the screener whether the threat is real and then records the screener's performance in a database that could be analyzed for performance trends.

maintaining, and enhancing screener performance, they only recently began reactivating TIP on a wide-scale basis because of competing priorities, a lack of training, and a lack of resources needed to deploy TIP activation teams. As TIP becomes operational at each airport, TSA headquarters and federal security directors[11] will have the capability to query and analyze performance data in a number of ways, including by individual screeners, checkpoints, terminals, and airports. TIP is expected to be fully deployed and operational by April 2004.

When fully deployed, the annual screener recertification test results will provide another source of data on screener performance. ATSA requires that TSA collect performance information on each screener through conducting an annual proficiency review to ensure he or she continues to meet all qualifications and standards required to perform the screening function. Although TSA began deploying federal screeners to airports in April 2002, TSA only recently began implementing the annual recertification program and does not expect to complete testing at all airports until March 2004. The recertification testing is comprised of three components: (1) image recognition; (2) knowledge of standard operating procedures; and (3) practical demonstration of skills, to be administered by a contractor. TSA officials consider 28,000 screeners as having completed the first two components because they successfully passed competency tests TSA administered at many airports as part of a screener workforce reduction effort. However, these competency tests did not include the third component of TSA's planned annual screener recertification program—the practical demonstration of skills. TSA officials awarded a contract for this component of the annual proficiency reviews in September 2003.

TSA's Performance Management Information System for passenger and baggage screening operations is also designed to collect performance data, but currently it contains limited information on screener performance in detecting threat objects. The Performance Management Information System collects a wide variety of metrics on workload, staffing, and equipment and is used to identify some performance indicators, such as the level of absenteeism, the average time for equipment repairs, and the status of TSA's efforts to meet goals for 100 percent electronic baggage

[11]Federal security directors oversee security at each of the nation's commercial airports.

screening.[12] However, the system does not contain any performance metrics related to the effectiveness of passenger screening. TSA is planning to integrate performance information from various systems into the Performance Management Information System to assist the agency in making strategic decisions. TSA further plans to continuously enhance the system as it learns what data are needed to best manage the agency. In addition to making improvements to the Performance Management Information System, TSA is currently developing performance indexes for both individual screeners and the screening system as a whole. The screener performance index will be based on data such as the results of training and recertification tests, and the index for the screening system will be based on information such as TIP results. TSA has not yet fully established its methodology for developing the indexes, but it expects to have them developed by the end of fiscal year 2004.

Performance Evaluation Tools under Development

TSA has recognized the need to strengthen the assessment of its performance, and it has initiated efforts to develop and implement strategic and performance plans to clarify goals, establish performance measures, and evaluate the performance of its security initiatives. Strategic plans are the starting point for an agency's planning and performance measurement efforts. Strategic plans include a comprehensive mission statement based on the agency's statutory requirements, a set of outcome-related strategic goals, and a description of how the agency intends to achieve these goals. The Government Performance and Results Act (GPRA)[13] establishes a framework for strategic plans that requires agencies to:

- clearly establish results-oriented performance goals in strategic and annual performance plans for which they will be held accountable,

[12]The Performance Management Information System also contains metrics on human resources, sizing, checkpoint, feedback, and incidents.

[13]The Government Performance and Results Act of 1993 shifts the focus of government operations from process to results by establishing a foundation for examining agency mission, performance goals and objectives, and results. Under the act, agencies are to prepare 5-year strategic plans that set the general direction for their efforts, and annual performance plans that establish connections between the long-term strategic goals outlined in the strategic plans and the day-to-day activities of managers and staff. Finally, the act requires that each agency report annually on the extent to which it is meeting its annual performance goals and the actions needed to achieve or modify those goals that have not been met.

- measure progress toward achieving those goals,
- determine the strategies and resources needed to effectively accomplish the goals,
- use performance information to make programmatic decisions necessary to improve performance, and
- formally communicate results in performance reports.

Although the Department of Homeland Security plans to issue one strategic plan for the department, it plans to incorporate strategic planning efforts from each of its component agencies. TSA recently completed a draft of its input into the Department of Homeland Security's strategic plan. TSA officials stated that the draft is designed to ensure their security initiatives are aligned with the agency's goals and objectives and that these initiatives represent the most efficient use of their resources. TSA officials submitted the draft plan to stakeholders in September 2003 for their review and comment. The Department of Homeland Security plans to issue its strategic plan by the end of the year.[14]

In addition to developing a strategic plan, TSA is developing a performance plan to help it evaluate the current effectiveness and levels of improvement in its programs, based on established performance measures. TSA submitted to the Congress a short-term performance plan in May 2003, as required by ATSA, that included performance goals and objectives. The plan also included an initial set of 32 performance measures, including the percentage of bags screened by explosive detection systems and the percentage of screeners in compliance with training standards. However, these measures were primarily output-based (measuring whether specific activities were achieved) and did not

[14]TSA is also developing a National Transportation Security System Plan, a draft of which is currently under review within TSA. TSA plans to promote consistent and mutually supporting intermodal planning in cooperation with administrators and in collaboration with key stakeholders from all modes of transportation. TSA designed the plan for use by agencies, owners, and operators of the transportation system to guide them as they develop their individual security plans. Accordingly, the National Transportation System Security Plan will include national modal plans to capture and tailor transportation security requirements for each mode of transportation, with particular emphasis on intermodal connections. Each modal plan will focus on security for people (workforce and passengers), cargo (baggage and shipments), infrastructure (vehicles, facilities, and right of ways), and response preparedness.

measure the effectiveness of TSA's security initiatives. TSA officials acknowledge that the goals and measures included in the report were narrowly focused and that in moving forward additional performance-based measures are needed.

In addition to developing a short-term performance plan, ATSA also requires that TSA develop a 5-year performance plan and annual performance report, including an evaluation of the extent to which its goals and objectives were met. TSA is currently developing performance goals and measures as part of its annual planning process and will collect baseline data throughout fiscal year 2004 to serve as a foundation for its performance targets. TSA also plans to increase its focus on measuring the effectiveness of various aspects of the aviation security system in its 5-year performance plan. According to TSA's current draft strategic plan, which outlines its overall goals and strategies for fiscal years 2003 through 2008, its efforts to measure the effectiveness of the aviation security system will include:

- random and scheduled reviews of the efficiency and effectiveness of security processes;
- oversight of compliance with security standards and approved programs through a combination of inspections, testing, interviews, and record reviews—to include TIP;
- measurement of performance against standards to ensure expected standards are met to drive process improvements; and
- collection and communication of performance data using a state-of-the-art data collection and reporting system.

In our January 2003 report on TSA's actions and plans to build a results-oriented culture, we recommended next steps that TSA should take to strengthen its strategic planning efforts.[15] These steps include establishing security performance goals and measures for all modes of transportation that involves stakeholders, and applying practices that have been shown to provide useful information in agency performance plans. We also identified practices that TSA can apply to ensure the usefulness of its required 5-year performance plan to TSA managers, the Congress, and

[15]U.S. General Accounting Office, *Transportation Security Administration: Actions and Plans to Build a Results-Oriented Culture*, GAO-03-190 (Washington, D.C.: Jan. 17, 2003).

other decision makers or interested parties. Table 1 outlines the practices we identified for TSA.

Table 1: Summary of Opportunities to Help Ensure Useful Annual Plans and Applied Practices

Opportunities to help ensure useful annual plans	Applied practices
Articulate a results orientation	1. Create a set of performance goals and measures that addresses important dimensions of program performance and balances competing priorities.
	2. Use intermediate goals and measures to show progress or contribution to intended results.
	3. Include explanatory information on the goals and measures.
	4. Develop performance goals to address mission-critical management problems.
	5. Show baseline and trend data for past performance.
	6. Identify projected target levels of performance for multiyear goals.
	7. Link the goals of component organizations to departmental strategic goals.
Coordinate cross-cutting programs	8. Identify programs that contribute to the same or similar results.
	9. Set complementary performance goals to show how differing program strategies are mutually reinforcing and establish common or complementary performance measures, as appropriate.
	10. Describe—briefly or refer to a separate document—planned coordination strategies.
Show how strategies will be used to achieve goals	11. Link strategies and programs to specific performance goals and describe how they will contribute to the achievement of those goals.
	12. Describe strategies to leverage or mitigate the effects of external factors on the accomplishment of performance goals.
	13. Discuss strategies to resolve mission-critical management problems.
	14. Discuss—briefly or refer to a separate plan—plans to ensure that mission-critical processes and information systems function properly and are secure.
Show performance consequences of budget and other resource decisions	15. Show how budgetary resources relate to the achievement of performance goals.
	16. Discuss—briefly and refer to the agency capital plan—how proposed capital assets (specifically information technology investments) will contribute to achieving performance goals.
	17. Discuss—briefly or refer to a separate plan—how the agency will use its human capital.
Build the capacity to gather and use performance information	18. Identify internal and external sources of data.
	19. Describe efforts to verify and validate performance data.
	20. Identify actions to compensate for unavailable or low-quality data.
	21. Discuss implications of data limitations for assessing performance.

Source: GAO.

TSA agreed with our recommendations and plans to incorporate these principles into its 5-year performance plan and annual performance report.

TSA plans to complete its 5-year performance plan and annual performance report by February 2004, as required by GPRA.

The Congress has also recognized the need for TSA to measure the effectiveness of its security initiatives and, as part of the Federal Aviation Administration's (FAA) reauthorization act—Vision 100: Century of Aviation Reauthorization Act—is currently considering a provision that would require the Secretary of the Department of Homeland Security to conduct a study of the effectiveness of the aviation security system.

Challenges in Strengthening TSA's Passenger Screening Program

In addition to collecting performance data on the effectiveness of its passenger screening program, TSA can strengthen other areas of the program to help improve screeners' ability to detect threat objects. In our September 2003 report that discussed our preliminary observations on TSA's passenger screening program, we noted that TSA can strengthen recurrent and supervisory training, staffing of screeners, and oversight of its contract screener pilot program. Since that report was issued, TSA has identified a number of actions it has taken or plans to take to address these concerns. We will be reviewing TSA's efforts to address these challenges as part of our ongoing review of this program.

Recurrent and Supervisory Training Programs Not Fully Developed

In fulfilling its passenger screening mandate, TSA must ensure that screeners are adequately trained and sufficiently skilled in identifying threat or dangerous objects at screening checkpoints. To help accomplish this, TSA has developed and deployed basic and remedial screener training programs. Basic screener training consists of 40 hours of classroom instruction and 60 hours of on-the-job training that screeners must successfully complete prior to making independent screening decisions. Additionally, TSA requires remedial training for any screener who fails an operational test and prohibits screeners from performing the screening function related to the test they failed until they successfully complete remedial training. TSA screening supervisors may also require remedial training for screeners they observe needing strengthening of their skills.

Although TSA has deployed basic and remedial training programs, it has not fully developed or deployed recurrent or supervisory training programs to ensure that screeners are effectively trained and supervised. Recurrent training—the ongoing training of screeners on a frequent basis—is critical in maintaining and enhancing screener skills. Although TSA has not fully developed a recurrent training program, it is in the process of deploying six recurrent training modules and is pilot testing an

Online Learning Management System for recurrent training comprised of about 360 components. TSA officials said that budget limitations had delayed implementation of the recurrent training modules and the online learning system.

Similarly, TSA has not fully developed or deployed a supervisory training program, even though it describes its screening supervisors as the key to a strong defense in detecting threat objects. However, TSA is taking steps in developing such a program, including working with the U.S. Department of Agriculture's Graduate School to tailor its off-the-shelf supervisory course to meet the specific training needs of TSA's screening supervisors. TSA reported that it is sending supervisors to the U.S. Department of Agriculture off-the-shelf supervisory course until the customized course is fielded in 2004. TSA also plans to establish a technical supervisor training component for recurrent training.

TSA Continues to Work to Identify Appropriate Staffing Levels at Airports

To conduct passenger and baggage screening functions at the nation's airports, TSA hired about 56,000 screeners. Initially, screener staff levels for all airports was developed by TSA headquarters without active input from the agency's federal security directors who are responsible for overseeing security at each of the nation's commercial airports. This has led to staffing imbalances, and concern by federal security directors that they had limited authority to respond to airport-specific staffing needs, such as reacting to fluctuations in daily and seasonal passenger flow. TSA officials acknowledged that their initial staffing efforts created imbalances in the screener workforce, and reported that as they work to further reduce the screener workforce,[16] they will solicit input from the Federal Security Directors as well as airport and air carrier officials. TSA has also

[16]TSA's screener workforce totaled 55,600 on March 31, 2003. The agency cut 3,000 positions for a screener workforce of 52,600 by June 1, 2003. An additional 3,000 positions were cut for a workforce of 49,600 full-time equivalents (FTE) by September 30, 2003, the end of the fiscal year. TSA officials predicted that the screener staffing level will be down to 45,000 by the end of fiscal year 2004. Beginning with the enactment of the 2002 Supplemental Appropriations Act for Further Recovery from and Response to Terrorist Attacks on the United States, Public Law 107-206 (August 2, 2002), and in subsequent appropriations acts, there have been restrictions on TSA impacting staffing levels. The current fiscal year 2004 Department of Homeland Security Appropriations Act, Public Law 108-90, contains a provision requiring that none of the funds in the act be used to recruit or hire personnel into TSA, which would cause the agency to exceed a screener staffing level of 45,000 full-time equivalents.

taken steps such as authorizing the hiring of part-time screeners at over 200 airports—the first of whom began working in September 2003.

To better address airport-specific staffing needs and accomplish workforce reduction goals, TSA developed its current screener staffing levels using a computer-based modeling process that took into account the number of screening checkpoints and lanes at an airport; originating passengers; the number of airport workers requiring screening; projected air carrier service increases and decreases during the year; and hours needed to accommodate screener training, leave, and breaks. TSA recently hired an outside consultant to conduct a study of screener staffing levels at various airports. TSA officials stated that they will continue to review the staffing allocation process through the modeling efforts to assess air carrier and airport growth patterns, and adjustments will be made as appropriate. We will continue to review TSA's staffing efforts as part of our ongoing review.

Assessment of Contract Screening Pilot Program

Consistent with ATSA, TSA implemented a pilot program using contract screeners at five commercial airports. The purpose of the 2-year pilot program is to determine the feasibility of using private screening companies rather than federal screeners. TSA initially required private screening companies to adhere to all of the procedures and protocols used by federal screeners. As a result, these airports had limited flexibility in running screening operations. However, TSA recently provided the contractors with some flexibility, such as allowing them to determine and maintain their own staffing levels and to make independent hiring decisions. ATSA gives all airport operators the option of applying to change from using federal screeners to using private screeners beginning in November 2004.

TSA has not yet determined how to evaluate and measure the performance of the pilot program airports or determine the feasibility of using contract screening companies. TSA recently awarded a contract to BearingPoint, Inc., to compare the performance of pilot screening with federal screening, including the overall strengths and weaknesses of both systems, and determine the reasons for any differences.[17] The evaluation is scheduled to

[17]According to the August 8, 2003, request for quotation for the evaluation of the contract screening pilot program, BearingPoint must include informed performance comparisons, both quantitative and qualitative, of private versus federal screeners overall and within different sizes and categories of airports.

be completed by March 31, 2004.[18] TSA has acknowledged that designing an effective evaluation of the screeners at the pilot airports will be challenging because key operational areas, including training, assessment, compensation, and equipment, have to a large extent been held constant across all airports, and therefore are not within the control of the private screening companies.[19] In its request for proposal for the pilot airport evaluation, TSA identified several data sources for the evaluation, including the Performance Management Information System and the Office of Internal Affairs and Program Review's covert testing of passenger screeners. However, as we recently reported, data from these systems in measuring the effectiveness of screening operations is limited. As a result, it will be a challenge for TSA to effectively compare the performance of the contract pilot airports with that of airports using federal screeners.

In conjunction with this evaluation, TSA will need to plan for the possible transition of airports from a federal system to a private screening company. Numerous airport operators have expressed an interest in obtaining more information to assist in their decision regarding using private screeners. Specifically, airport operators stated that they would like to determine who would bear responsibility for funding the screening contract, airport liability in the event of an incident linked to a screener failure, how well the current pilot program airports are performing, performance standards to which contract screeners would be held, and TSA's role in overseeing contracted screening. If airports are permitted to opt out of using federal screeners, this could have a significant impact on TSA's role in overseeing the screening function as well as the number of federal screeners needed.

[18]Based on the time frames established in the request for quotation, BearingPoint, Inc. is required to develop a project plan and evaluation model no later than December 12, 2003.

[19]TSA's request for proposal for the pilot program evaluation notes that there are a significant number of operational and managerial elements at the discretion of the private screening companies that should be considered in the evaluation, including supervision, overhead, materials, recruiting, and scheduling.

TSA Faces Additional Programmatic and Management Challenges

In addition to the challenges it faces in conducting its passenger screening program and assessing program effectiveness, TSA faces a number of other programmatic and management challenges in strengthening aviation security. These challenges include implementing the new Computer-Assisted Passenger Prescreening System; strengthening baggage screening, airport perimeter and access controls, air cargo, and general aviation security; managing the costs of aviation security initiatives; and managing human capital. TSA has been addressing these challenges through a variety of efforts. We have work in progress that is examining TSA's efforts in most of these areas, and we will be reporting on TSA's progress in the future.

Computer-Assisted Passenger Prescreening System (CAPPS II)

TSA is developing a new Computer-Assisted Passenger Prescreening System, or CAPPS II. This system is intended to replace the current Computer-Assisted Passenger Screening program, which was developed in the mid-1990s by the Federal Aviation Administration to enable air carriers to identify passengers requiring additional security attention. The current system is maintained as a part of the airlines' reservation systems and, operating under federal guidelines, uses a number of behavioral characteristics to select passengers for additional screening.

In the wake of the September 11, 2001, terrorist attacks, a number of weaknesses in the current prescreening program were exposed. For example, although the characteristics used to identify passengers for additional screening are classified, several have become public knowledge through the press or on the Internet. Although enhancements have been made to address some of these weaknesses, the behavioral traits used in the system may not reflect current intelligence information. It is also difficult to quickly modify the system to respond to real-time changes in threats. Additionally, because the current system operates independently within each air carrier reservation system, changes to each air carrier's system to modify the prescreening system can be costly and time-consuming.

In contrast, CAPPS II is planned to be a government-run program that will provide real-time risk assessment for all airline passengers. Unlike the current system, TSA is designing CAPPS II to identify and compare personal information with commercially available data to confirm a passenger's identity. The system will then run the identifying information against government databases and generate a "risk" score for the passenger. The risk score will determine the level of screening that the passenger will undergo before boarding. TSA currently estimates that

initial implementation of CAPPS II will occur during the fall of 2004, with full implementation expected by the fall of 2005.

TSA faces a number of challenges that could impede its ability to implement CAPPS II. Among the most significant are the following:

- concerns about travelers' privacy rights and the safeguards established to protect passenger data;
- the accuracy of the databases being used by the CAPPS II system and whether inaccuracies could generate a high number of false positives and erroneously prevent or delay passengers from boarding their flights;
- the length of time that data will be retained by TSA;
- the availability of a redress process through which passengers could get erroneous information corrected;
- concerns that identify theft, in which someone steals relevant data and impersonates another individual to obtain that person's low risk score, may not be detected and thereby negate the security benefits of the system; and
- obtaining the international cooperation needed for CAPPS II to be fully effective, as some countries consider the passenger information required by CAPPS II as a potential violation of their privacy laws.

We are currently assessing these and other challenges in the development and implementation of the CAPPS II system and expect to issue a final report on our work in early 2004.

Checked Baggage Screening

Checked baggage represents a significant security concern, as explosive devices in baggage can, and have, been placed in aircraft holds. ATSA required screening of all checked baggage on commercial aircraft by December 31, 2002, using explosive detection systems to electronically scan baggage for explosives. According to TSA, electronic screening can be accomplished by bulk explosives detection systems (EDS)[20] or

[20]Explosives detection systems use probing radiation to examine objects inside baggage and identify the characteristic signatures of threat explosives. EDS equipment operates in an automated mode.

explosives trace detection (ETD) systems.[21] However, TSA faced challenges in meeting the mandated implementation date. First, the production capabilities of EDS manufacturers were insufficient to produce the number of units needed. Additionally, according to TSA, it was not possible to undertake all of the airport modifications necessary to accommodate the EDS equipment in each airport's baggage-handling area. In order to ensure that all checked baggage is screened, TSA established a program that uses alternative measures, including explosives-sniffing dogs, positive passenger bag match,[22] and physical hand searches at airports where sufficient EDS or ETD technology was not available. Section 425 of the Homeland Security Act allowed the Under Secretary for Transportation Security to grant airports unable to meet the December 31, 2002, 100 percent screening deadline an extension until December 31, 2003. Although TSA has made progress in implementing EDS technology at more airports, it has reported that it will not meet the revised mandate for 100 percent electronic screening of all checked baggage. Specifically, as of October 2003, TSA reported that it will not meet the deadline for electronic screening by December 31, 2003, at five airports. Airport representatives with whom we spoke expressed concern that there has not been enough time to produce, install, and integrate all of the systems required to meet the deadline.

In addition to fielding the EDS systems at airports, difficulties exist in integrating these systems into airport baggage-handling systems. For those airports that have installed EDS equipment, many have been located in airport lobbies as stand-alone systems. The chief drawback of stand-alone systems is that because of their size and weight there is a limit to the number of units that can be placed in airport lobbies, and numerous screeners are required to handle the checked bags because each bag must be physically conveyed to the EDS machines and then moved back to the conveyor system for transport to the baggage-handling room in the air terminal. Some airports are in the process of integrating the EDS equipment inline with the conveyor belts that transport baggage from the ticket counter to the baggage-handling area. However, the reconfiguring of airports for in-line checked baggage screening can be extensive and

[21]Explosive trace detection works by detecting vapors and residues of explosives. Human operators collect samples by rubbing bags with swabs, which are chemically analyzed to identify any traces of explosive materials.

[22]Positive passenger bag match is an alternative method of screening checked baggage, which requires that the passenger be on the same aircraft as the checked baggage.

costly.[23] TSA has reported that in-line EDS equipment installation costs range from $1 million to $3 million per piece of equipment. In February 2003, we identified letters of intent[24] as a funding option that has been successfully used to leverage private sources of funding.[25] TSA has since written letters of intent covering seven airports promising multiyear financial support totaling over $770 million for in-line integration of EDS equipment.[26] Further, TSA officials have stated that they have identified 25 to 35 airports as candidates for further letters of intent pending Congressional authorization of funding. We are examining TSA's baggage screening program, including its issuance of letters of intent, in an ongoing assignment.

Perimeter and Access Controls

Prior to September 2001, work performed by GAO and others highlighted the vulnerabilities in controls for limiting access to secure airport areas. In one report, we noted that GAO special agents were able to use fictitious law enforcement badges and credentials to gain access to secure areas, bypass security checkpoints, and walk unescorted to aircraft departure gates.[27] The agents, who had been issued tickets and boarding passes, could have carried weapons, explosives, or other dangerous objects onto aircraft. Concerns over the adequacy of the vetting process for airport workers who have unescorted access to secure airport areas have also arisen, in part as a result of federal agency airport security sweeps that uncovered hundreds of instances in which airport workers lied about their

[23]In-line screening involves incorporating EDS machines into airport baggage handling systems to improve throughput of baggage and to streamline airport operations.

[24]A letter of intent represents a nonbinding commitment from an agency to provide multiyear funding to an entity beyond the current authorization period. Thus, that letter allows an airport to proceed with a project without waiting for future federal funds because the airport and investors know that allowable costs are likely to be reimbursed.

[25]U.S. General Accounting Office, *Airport Finance: Past Funding Levels May Not Be Sufficient to Cover Airports' Planned Capital Development*, GAO-03-497T (Washington, D.C.: Feb. 25, 2003).

[26]The seven airports include Denver International Airport, Las Vegas McCarran International Airport, Los Angeles International Airport, Ontario International Airport, Seattle/Tacoma International Airport, Dallas/Fort Worth International Airport, and Boston Logan International Airport. The purpose is to help defray the costs of installing permanent explosive detection systems that are integrated with airports' checked baggage conveyor systems.

[27]U.S. General Accounting Office, *Security: Breaches at Federal Agencies and Airports*, GAO/T-OSI-00-10 (Washington, D.C.: May 25, 2000).

criminal history, or immigration status, or provided false or inaccurate Social Security numbers on their application for security clearances to obtain employment.

ATSA contains provisions to improve perimeter access security at the nation's airports and strengthen background checks for employees working in secure airport areas, and TSA has made some progress in this area. For example, federal mandates were issued to strengthen airport perimeter security by limiting the number of airport access points, and they require random screening of individuals, vehicles, and property before entry at the remaining perimeter access points. Further, TSA made criminal history checks mandatory for employees with access to secure or sterile airport areas. To date, criminal history checks have been conducted on approximately 1 million of these employees. TSA also has plans to develop a pilot airport security program and is reviewing security technologies in the areas of biometrics access control identification systems (i.e., fingerprints or iris scans), anti-piggybacking technologies (to prevent more than one employee from entering a secure area at a time), and video monitoring systems for perimeter security. TSA solicited commercial airport participation in the program. It is currently reviewing information from interested airports and plans to select 20 airports for the program.

Although progress has been made, challenges remain with perimeter security and access controls at commercial airports. Specifically, ATSA contains numerous requirements for strengthening perimeter security and access controls, some of which contained deadlines, which TSA is working to meet. In addition, a significant concern is the possibility of terrorists using shoulder-fired portable missiles from locations near the airport. We reported in June 2003 that airport operators have increased their patrols of airport perimeters since September 2001, but industry officials stated that they do not have enough resources to completely protect against missile attacks.[28] A number of technologies could be used to secure and monitor airport perimeters, including barriers, motion sensors, and closed-circuit television. Airport representatives have cautioned that as security enhancements are made to airport perimeters, it will be important for TSA to coordinate with the Federal Aviation Administration and the airport operators to ensure that any enhancements

[28]U.S. General Accounting Office, *Transportation Security: Federal Action Needed to Help Address Security Challenges*, GAO-03-843 (Washington, D.C.: June 30, 2003).

do not pose safety risks for aircraft. To further examine these threats and challenges, we have ongoing work assessing TSA's progress in meeting ATSA provisions related to improving perimeter security, access controls, and background checks for airport employees and other individuals with access to secure areas of the airport, as well as the nature and extent of the threat from shoulder-fired missiles.

Air Cargo Security

As we and the Department of Transportation's Inspector General have reported, vulnerabilities exist in ensuring the security of cargo carried aboard commercial passenger and all-cargo aircraft. TSA has reported that an estimated 12.5 million tons of cargo are transported each year—9.7 million tons on all-cargo planes and 2.8 million tons on passenger planes. Potential security risks are associated with the transport of air cargo—including the introduction of undetected explosive and incendiary devices in cargo placed aboard aircraft. To reduce these risks, ATSA requires that all cargo carried aboard commercial passenger aircraft be screened and that TSA have a system in place as soon as practicable to screen, inspect, or otherwise ensure the security of cargo on all-cargo aircraft. Despite these requirements, it has been reported that less than 5 percent of cargo placed on passenger airplanes is physically screened.[29] TSA's primary approach to ensuring air cargo security and safety is to ensure compliance with the "known shipper" program—which allows shippers that have established business histories with air carriers or freight forwarders to ship cargo on planes. However, we and the Department of Transportation's Inspector General have identified weaknesses in the known shipper program and in TSA's procedures for approving freight forwarders, such as possible tampering with freight at various handoff points before it is loaded into an aircraft.[30]

Since September 2001, TSA has taken a number of actions to enhance cargo security, such as implementing a database of known shippers in October 2002. The database is the first phase in developing a cargo profiling system similar to the Computer-Assisted Passenger Prescreening System. However, in December 2002, we reported that additional operational and technological measures, such as checking the identity of

[29]Congressional Research Service, *Air Cargo Security*, September 11, 2003.

[30]U.S. General Accounting Office, *Aviation Security: Vulnerabilities and Potential Improvements for the Air Cargo System*, GAO-03-344 (Washington, D.C.: Dec. 20, 2002).

individuals making cargo deliveries, have the potential to improve air cargo security in the near term.[31] We further reported that TSA lacks a comprehensive plan with long-term goals and performance targets for cargo security, time frames for completing security improvements, and risk-based criteria for prioritizing actions to achieve those goals. Accordingly, we recommended that TSA develop a comprehensive plan for air cargo security that incorporates a risk management approach, includes a list of security priorities, and sets deadlines for completing actions. TSA agreed with this recommendation and expects to develop such a plan by the end of 2003. It will be important that this plan include a timetable for implementation to help ensure that vulnerabilities in this area are reduced.

General Aviation Security

Since September 2001, TSA has taken limited action to improve general aviation security, leaving general aviation far more open and potentially vulnerable than commercial aviation. General aviation is vulnerable because general aviation pilots and passengers are not screened before takeoff and the contents of general aviation planes are not screened at any point. General aviation includes more than 200,000 privately owned airplanes, which are located in every state at more than 19,000 airports.[32] More than 550 of these airports also provide commercial service. In the last 5 years, about 70 aircraft have been stolen from general aviation airports, indicating a potential weakness that could be exploited by terrorists. This vulnerability was demonstrated in January 2002, when a teenage flight student stole and crashed a single-engine airplane into a Tampa, Florida skyscraper. Moreover, general aviation aircraft could be used in other types of terrorist acts. It was reported that the September 11th hijackers researched the use of crop dusters to spread biological or chemical agents.

We reported in September 2003 that TSA had chartered a working group on general aviation within the existing Aviation Security Advisory Committee.[33] The working group consists of industry stakeholders and is designed to identify and recommend actions to close potential security

[31] U.S. General Accounting Office, *Aviation Security: Progress since September 11, 2001, and the Challenges Ahead*, GAO-03-1150T (Washington, D.C.: September 9, 2003).

[32] Of the 19,000 general aviation airports, 5,400 are publicly owned. TSA is currently focusing its efforts on these publicly owned airports. TSA is still unclear about its role in inspecting privately owned general aviation airports.

[33] GAO-03-1150T.

gaps in general aviation. On October 1, 2003, the working group issued a report that included a number of recommendations for general aviation airport operators' voluntary use in evaluating airports' security requirements. These recommendations are both broad in scope and generic in their application, with the intent that every general aviation airport and landing facility operators may use them to evaluate that facility's physical security, procedures, infrastructure, and resources. TSA is taking some additional action to strengthen security at general aviation airports, including developing a risk-based self-assessment tool for general aviation airports to use in identifying security concerns. We have ongoing work that is examining general aviation security in further detail.

Aviation Security Funding

TSA faces two key funding and accountability challenges in securing the commercial aviation system: (1) paying for increased aviation security, and (2) ensuring that these costs are controlled. These challenges are particularly critical due to the government incurring large and increasing deficits. The rapid rise in needed funding for aviation security enhancements further exacerbates budget challenges. The costs associated with aviation security are huge. The Department of Homeland Security appropriation includes $3.7 billion for aviation security for fiscal year 2004. The passenger and baggage screening functions alone account for most of this funding, with about $1.8 billion appropriated for passenger screening and $1.3 billion for baggage screening. ATSA created passenger and air carrier security fees to pay for the costs of aviation security, but the fees have not generated enough money to do so. The Department of Transportation's Inspector General reported that the security fees are estimated to generate only about $1.7 billion during fiscal year 2004.

A major funding challenge is paying for the purchase and installation of the remaining explosives detection systems, including integration into airport baggage-handling systems. Integrating the equipment with the baggage-handling systems is expected to be costly because it will require major facility modifications. For example, modifications needed to integrate the equipment at Boston's Logan International Airport are estimated to cost $146 million. Modifications for Dallas/Fort Worth International Airport are estimated to cost $193 million. According to TSA and the Department of Transportation's Inspector General, the cost of integrating the equipment nationwide could be $3 billion.

A key question that must be addressed is how to pay for these installation costs. The Federal Aviation Administration's Airport Improvement Program (AIP) and passenger facility charges have been eligible sources

for funding this work.[34] During fiscal year 2002, AIP grant funds totaling $561 million were used for terminal modifications to enhance security. However, using these funds for security reduced the funding available for other airport development and rehabilitation projects. To provide financial assistance to airports for security-related capital investments, such as the installation of explosives detection equipment, proposed aviation reauthorization legislation would establish an aviation security capital fund that would authorize $2 billion over the next 4 years.

In February 2003, we identified letters of intent as a funding option that has been successfully used to leverage private sources of funding.[35] TSA has since signed letters of intent covering seven airports—Boston Logan, Dallas/Fort Worth, Denver, Los Angeles, McCarran (Las Vegas), Ontario (California), and Seattle/Tacoma international airports. Under the agreements, TSA will pay 75 percent of the cost of integrating the explosives detection equipment into the baggage-handling systems. The payments will stretch out over 3 to 4 years. TSA officials have identified more airports that would be candidates for similar agreements.

Another challenge is ensuring continued investment in transportation research and development. For fiscal year 2003, TSA was appropriated about $110 million for research and development, of which $75 million was designated for the next-generation explosives detection systems. However, TSA proposed to reprogram $61.2 million of these funds to be used for other purposes, leaving about $12.7 million to be spent on research and development in that year. This proposed reprogramming could limit TSA's ability to sustain and strengthen aviation security by continuing to invest in research and development for more effective equipment to screen passengers, their carry-on and checked baggage, and cargo. In ongoing work, we are examining the nature and scope of research and development work by TSA and the Department of Homeland Security, including their strategy for accelerating the development of transportation security technologies.

[34]The Airport Improvement Program trust fund is used to fund capital improvements to airports, including some security enhancements, such as terminal modifications to accommodate explosive detection equipment.

[35]GAO-03-497T.

Human Capital Management

As it organizes itself to protect the nation's transportation system, TSA faces the challenge of strategically managing its workforce of about 60,000 people—more than 80 percent of whom are passenger and baggage screeners. Additionally, over the next several years, TSA faces the challenge of sizing and managing this workforce as efficiency is improved with new security-enhancing technologies, processes, and procedures. For example, as explosives detection systems are integrated with baggage-handling systems, the use of more labor-intensive screening methods, such as trace detection techniques and manual bag searches, can be reduced. Other planned security enhancements, such as CAPPS II and a registered traveler program, also have the potential to make screening more efficient. Further, if airports opt out of the federal screener program and use their own or contract employees to provide screening instead of TSA screeners, a significant impact on TSA staffing could occur.

To assist agencies in managing their human capital more strategically, we have developed a model that identifies cornerstones and related critical success factors that agencies should apply and steps they can take.[36] Our model is designed to help agency leaders effectively lead and manage their people and integrate human capital considerations into daily decision making and the program results they seek to achieve. In January 2003, we reported that TSA was addressing some critical human capital success factors by using a wide range of tools available for hiring, and beginning to link individual performance to organizational goals.[37] However, concerns remain about the size and training of that workforce, the adequacy of the initial background checks for screeners, and TSA's progress in setting up a performance management system. TSA is currently developing a human capital strategy, which it expects to be completed by the end of this year.

TSA has proposed cutting the screener workforce by an additional 3,000 during fiscal year 2004. This planned reduction has raised concerns about passenger delays at airports and has led TSA to begin hiring part-time screeners to make more flexible and efficient use of its workforce. In addition, TSA used an abbreviated background check process to hire and deploy enough screeners to meet ATSA's screening deadlines during 2002. After obtaining additional background information, TSA terminated the

[36] U.S. General Accounting Office, *A Model of Strategic Human Capital Management*, GAO-02-373SP (Washington, D.C.: March 2002).

[37] U.S. General Accounting Office, *Major Management Challenges and Program Risks: Department of Transportation*, GAO-03-108 (Washington, D.C.: January 2003).

employment of some of these screeners. TSA reported 1,208 terminations as of May 31, 2003, that it ascribed to a variety of reasons, including criminal offenses and failures to pass alcohol and drug tests. Furthermore, the national media have reported allegations of operational and management control problems that emerged with the expansion of the Federal Air Marshal Service, including inadequate background checks and training, uneven scheduling, and inadequate policies and procedures. We reported in January 2003 that TSA had taken the initial steps in establishing a performance management system linked to organizational goals. Such a system will be critical for TSA to motivate and manage staff, ensure the quality of screeners' performance, and, ultimately, restore public confidence in air travel. In ongoing work, we are examining the effectiveness of TSA's efforts to train, equip, and supervise passenger screeners, and we are assessing the effects of expansion on the Federal Air Marshal Service.[38]

Concluding Observations

TSA faces many challenges in strengthening its passenger screening and other security programs. To best address these challenges, it needs the information and tools necessary to ensure that its efforts are effective, are appropriately focused, and are achieving expected results. Without knowledge on the effectiveness of its programs, TSA and the public have little assurance regarding the level of security provided, and whether TSA is using its resources to maximize security benefits. As TSA implements new security initiatives and addresses associated challenges, measuring program effectiveness will help it best focus on the areas of greatest need. We are encouraged that TSA is undertaking efforts to develop the information and tools needed to measure its performance.

Mr. Chairman, this concludes my statement. I would be pleased to answer any questions that you or other members of the Committee may have.

Contact Information

[38] The Federal Air Marshal Service has been transferred out of TSA and into the Department of Homeland Security's Bureau of Immigration and Customs Enforcement.

For further information on this testimony, please contact Cathleen A. Berrick at (202) 512-8777. Individuals making key contributions to this testimony include Mike Bollinger, Lisa Brown, Jack Schulze, and Maria Strudwick.

Related GAO Products

Aviation Security: Efforts to Measure Effectiveness and Address Challenges. GAO-04-232T. Washington, D.C.: November 5, 2003.

Airport Passenger Screening: Preliminary Observations on Progress Made and Challenges Remaining. GAO-03-1173. Washington, D.C.: September 24, 2003.

Aviation Security: Progress since September 11, 2001, and the Challenges Ahead. GAO-03-1150T. Washington, D.C.: September 9, 2003

Transportation Security: Federal Action Needed to Help Address Security Challenges. GAO-03-843. Washington, D.C.: June 30, 2003.

Transportation Security: Post-September 11th Initiatives and Long-Term Challenges. GAO-03-616T. Washington, D.C.: April 1, 2003.

Aviation Security: Measures Needed to Improve Security of Pilot Certification Process. GAO-03-248NI. Washington, D.C.: February 3, 2003. (NOT FOR PUBLIC DISSEMINATION)

Aviation Security: Vulnerabilities and Potential Improvements for the Air Cargo System. GAO-03-286NI. Washington, D.C.: December 20, 2002. (NOT FOR PUBLIC DISSEMINATION)

Aviation Security: Vulnerabilities and Potential Improvements for the Air Cargo System. GAO-03-344. Washington, D.C.: December 20, 2002.

Aviation Security: Vulnerability of Commercial Aviation to Attacks by Terrorists Using Dangerous Goods. GAO-03-30C. Washington, D.C.: December 3, 2002

Aviation Security: Registered Traveler Program Policy and Implementation Issues. GAO-03-253. Washington, D.C.: November 22, 2002.

Aviation Security: Transportation Security Administration Faces Immediate and Long-Term Challenges. GAO-03-971T. Washington, D.C.: July 25, 2002.

Aviation Security: Information Concerning the Arming of Commercial Pilots. GAO-02-822R. Washington, D.C.: June 28, 2002.

Aviation Security: Deployment and Capabilities of Explosive Detection Equipment. GAO-02-713C. Washington, D.C.: June 20, 2002. (CLASSIFIED)

Aviation Security: Information on Vulnerabilities in the Nation's Air Transportation System. GAO-01-1164T. Washington, D.C.: September 26, 2001. (NOT FOR PUBLIC DISSEMINATION)

Aviation Security: Information on the Nation's Air Transportation System Vulnerabilities. GAO-01-1174T. Washington, D.C.: September 26, 2001. (NOT FOR PUBLIC DISSEMINATION)

Aviation Security: Vulnerabilities in, and Alternatives for, Preboard Screening Security Operations. GAO-01-1171T. Washington, D.C.: September 25, 2001.

Aviation Security: Weaknesses in Airport Security and Options for Assigning Screening Responsibilities. GAO-01-1165T. Washington, D.C.: September 21, 2001.

Aviation Security: Terrorist Acts Demonstrate Urgent Need to Improve Security at the Nation's Airports. GAO-01-1162T. Washington, D.C.: September 20, 2001.

Aviation Security: Terrorist Acts Illustrate Severe Weaknesses in Aviation Security. GAO-01-1166T. Washington, D.C.: September 20, 2001.

Responses of Federal Agencies and Airports We Surveyed about Access Security Improvements. GAO-01-1069R. Washington, D.C.: August 31, 2001.

Responses of Federal Agencies and Airports We Surveyed about Access Security Improvements. GAO-01-1068R. Washington, D.C.: August 31, 2001. (RESTRICTED)

FAA Computer Security: Recommendations to Address Continuing Weaknesses. GAO-01-171. Washington, D.C.: December 6, 2000.

Aviation Security: Additional Controls Needed to Address Weaknesses in Carriage of Weapons Regulations. GAO/RCED-00-181. Washington, D.C.: September 29, 2000.

FAA Computer Security: Actions Needed to Address Critical Weaknesses That Jeopardize Aviation Operations. GAO/T-AIMD-00-330. Washington, D.C.: September 27, 2000.

FAA Computer Security: Concerns Remain Due to Personnel and Other Continuing Weaknesses. GAO/AIMD-00-252. Washington, D.C.: August 16, 2000.

Aviation Security: Long-Standing Problems Impair Airport Screeners' Performance. GAO/RCED-00-75. Washington, D.C.: June 28, 2000.

Aviation Security: Screeners Continue to Have Serious Problems Detecting Dangerous Objects. GAO/RCED-00-159. Washington, D.C.: June 22, 2000. (NOT FOR PUBLIC DISSEMINATION)

Security: Breaches at Federal Agencies and Airports. GAO-OSI-00-10. Washington, D.C.: May 25, 2000.

GAO's Mission

The General Accounting Office, the audit, evaluation and investigative arm of Congress, exists to support Congress in meeting its constitutional responsibilities and to help improve the performance and accountability of the federal government for the American people. GAO examines the use of public funds; evaluates federal programs and policies; and provides analyses, recommendations, and other assistance to help Congress make informed oversight, policy, and funding decisions. GAO's commitment to good government is reflected in its core values of accountability, integrity, and reliability.

Obtaining Copies of GAO Reports and Testimony

The fastest and easiest way to obtain copies of GAO documents at no cost is through the Internet. GAO's Web site (www.gao.gov) contains abstracts and full-text files of current reports and testimony and an expanding archive of older products. The Web site features a search engine to help you locate documents using key words and phrases. You can print these documents in their entirety, including charts and other graphics.

Each day, GAO issues a list of newly released reports, testimony, and correspondence. GAO posts this list, known as "Today's Reports," on its Web site daily. The list contains links to the full-text document files. To have GAO e-mail this list to you every afternoon, go to www.gao.gov and select "Subscribe to e-mail alerts" under the "Order GAO Products" heading.

Order by Mail or Phone

The first copy of each printed report is free. Additional copies are $2 each. A check or money order should be made out to the Superintendent of Documents. GAO also accepts VISA and Mastercard. Orders for 100 or more copies mailed to a single address are discounted 25 percent. Orders should be sent to:

U.S. General Accounting Office
441 G Street NW, Room LM
Washington, D.C. 20548

To order by Phone:	Voice:	(202) 512-6000
	TDD:	(202) 512-2537
	Fax:	(202) 512-6061

To Report Fraud, Waste, and Abuse in Federal Programs

Contact:

Web site: www.gao.gov/fraudnet/fraudnet.htm
E-mail: fraudnet@gao.gov
Automated answering system: (800) 424-5454 or (202) 512-7470

Public Affairs

Jeff Nelligan, Managing Director, NelliganJ@gao.gov (202) 512-4800
U.S. General Accounting Office, 441 G Street NW, Room 7149
Washington, D.C. 20548

PRINTED ON RECYCLED PAPER

Mr. SHAYS. Mr. DeMell.

Mr. DEMELL. Mr. Chairman, since November 2002, FirstLine Transportation Security has provided predeparture screening services for the TSA at Kansas City International Airport. Under the PP5 pilot program, FirstLine must meet the same overall hiring, training and security requirements as Federal screeners. Our employees receive training from the TSA to ensure that security measures are consistent with the TSA procedures.

We firmly believe that FirstLine and the TSA must form a seamless partnership. Make no mistake the TSA must continue to provide supervision and accountability for overall safety standards and hiring practices. However, the pilot site should not be required to mirror every procedure used at non-PP5 airports for the sake of sameness alone. The second year of the PP5 program should give private screening contractors sufficient flexibility to implement private sector innovations and creativity which could lead to higher passenger security at the most efficient cost to the taxpayer.

To help measure progress, it is essential to recall how the pre-September 11 screening process worked. Security was treated just like any other airline contract or commodity, resulting in a minimum wage work environment and atmosphere. The selection of equipment used at checkpoints reflected budgetary caution rather than safety concerns. Financial incentive clearly tilted toward making checkpoint passenger screening just another line item to be constantly squeezed into an already financially challenged industry. All of this changed after September 11 with the creation of the TSA.

This new security screening model, which included the PP5 program, has not been without its challenges. On October 8, 2002, the TSA awarded FirstLine a PP5 program contract. Just 42 days later, right before the holiday rush, FirstLine assumed control for meeting the staffing requirements for KCI screening. It soon became evident that the PP5 program was not at the top of the TSA's to-do list. FSDs were forced to administer a new program, apparently without sufficient headquarters direction or support.

One of the major problems we experienced is that the TSA involved too many contractors performing too many tasks under inflexible contracting arrangements. For example, FirstLine can only hire individuals who pass TSA's assessment and training criteria. This qualification process is run by TSA contractors who appear to be limited to either the number of individuals they can assess or train as well as to the amount of time they can spend at KCI. It was a full 8 months before TSA's contractors made a repeat assessment and training process available to FirstLine. This inability to fill vacancies severely frustrated our operations and continues to be an unresolved hurdle.

Despite these challenges, we are particularly proud of the work that our employees perform given an airport configuration that requires 12 screening checkpoints. By comparison, Atlanta Hartsfield has only four. The KCI layout also requires us to double-screen many passengers who must leave the secure area for restrooms or food. We have developed a close working relationship with Richard Curasi, KCI's Federal Security Director, to ensure that KCI security responsibilities are met. His central focus on our shared secu-

rity mission and his personal efforts to foster a true partnership are critical to the success of this evolving public-private screening level.

Our ability to bring private sector human services management enhances the screening product we deliver. FirstLine can provide enhanced pay scales, training and rewards for exceptional performance and attendance in excess of government requirements. Our Employee Advisory Committee allows management responsiveness to employee concerns in real time, and we also have the ability to discipline or offer corrective guidance in a timely manner. At KCI, we remove the TSA's burden of day-to-day resource management, allowing the Federal Government to focus on security, safety and technology priorities.

Finally, there are a number of adjustments that could be incorporated into the PP5 program that would in no way compromise the high security standards we fully support. Two examples include increasing local decisionmaking ability at the FSD and contractor level regarding assessment, training and passenger traffic scheduling requirements, all of which are critical to maintaining appropriate staff levels and controlling overtime; and providing funding support for software management tools that enable maximum work force utilization as well as maintenance of employee performance and training records.

Mr. Chairman, our PP5 experience has convinced us that the private sector has much to offer TSA and the Nation in our post-September 11 screening approach. With appropriate modifications to the PP5 program, these contributions could be even more easily identified and measured in the coming year. FirstLine is committed to ensuring that the second year of the PP5 and our work for the traveling public at KCI continues to enhance the security of our airline passenger system.

Thank you.

Mr. SHAYS. Thank you, Mr. DeMell.

[The prepared statement of Mr. DeMell follows:]

WRITTEN TESTIMONY OF

JOHN DEMELL
PRESIDENT
FIRSTLINE TRANSPORTATION SECURITY, INC.

BEFORE THE

COMMITTEE ON GOVERNMENT REFORM
U.S. HOUSE OF REPRESENTATIVES

REVIEW OF AIRLINE PASSENGER SCREENER
TRAINING, TESTING, AND SUPERVISION

NOVEMBER 20, 2003

Written Testimony of John DeMell
FirstLine Transportation Security, Inc.
November 20, 2003

Chairman Davis, Ranking Member Waxman, and Members of the Committee, thank you for the opportunity to assist the Committee's important review of the current airline passenger and baggage screening process.

Overview

Since November 2002, FirstLine Transportation Security, Inc. ("FirstLine") and our nearly 700 professional employees have provided pre-departure passenger and baggage screening services for the Transportation Security Administration ("TSA") and the traveling public at Kansas City International Airport ("KCI"). On a recent site visit, then-TSA Administrator Adm. James Loy stated that the FirstLine-TSA KCI screening partnership is going "very, very well."

FirstLine is a subsidiary of SMS Holdings, a privately-owned company with a fifteen year history of providing security, aviation, and facility maintenance services across the nation. In April 2002, through a bankruptcy purchase, SMS acquired the management team and certain assets (excluding pre-board screening contracts) of International Total Services, Inc. ("ITS"), a company that for over twenty years had provided passenger screening and airline services across the U.S.

The SMS family of companies also includes Valor Security Services, with employees protecting over 160 enclosed shopping malls in 32 states; Service Management Systems, a leading provider of facility services management to multi-use facilities in 32 states; and PrimeFlight Aviation Services, whose 4,000 employees provide airside and landside services in 60 airports nationwide.

Under the Aviation and Transportation Security Act ("Act"), the TSA assumed responsibility for pre-board screening of passengers and luggage at all U.S. airports. In addition, as required by Congress, the TSA implemented a pilot program using private contract screeners in lieu of federal screeners at five commercial airports (Kansas City, MO; San Francisco, CA; Rochester, NY; Tupelo, MS; and Jackson Hole, WY) to determine the feasibility of using private screening companies in concert with federal oversight. The five selected airports represent a facility in each airport category.

Under the pilot program, which has come to be known as the "PP5 program," private screening contractors must meet the same overall hiring, training, and security requirements as those locations employing federal screeners. The employees of the PP5 contractors receive training from the TSA and work closely with the TSA site managers to ensure that security measures are consistent with the TSA's procedures. In addition, private screeners receive enhanced professional training from the private entities, such as FirstLine.

Now entering its second year, the TSA's PP5 program ideally will provide valuable data and insight to Congress, the TSA, and airport operators on the feasibility and complementary effectiveness of using private screening firms under federal government oversight and strict adherence to the federal airport security guidelines.

Today, FirstLine is very pleased to provide the Committee with our perspective on the shift from the pre-9/11 screening model, our experience as one of the PP5 private sector contractors, and our observations on key opportunities that, if implemented in the PP5 program, would continue to strengthen airline passenger and baggage screening in the months ahead.

To maximize the benefits of the pilot program:

- Private screening contractors and the TSA must form a seamless, cooperative, and mission-sensitive partnership.
- The TSA must continue to provide supervision and accountability for overall safety standards and hiring practices, which require high caliber airport screeners paid at federally determined minimum compensation levels.
- However, while working within these parameters, private screening contractors at the pilot sites must not be required to identically mirror every procedure used at airport locations employing federal screeners, simply for the sake of "sameness."
- Rather, as Congress intended, the pilot project should truly serve as a test of the private sector airport security screening concept by giving private screening contractors sufficient flexibility to implement private sector innovations and creativity, which could lead to higher passenger security at the most efficient cost to the taxpayer.

The Pre-9/11 World

The deeply tragic events of September 11, 2001, forever changed passenger screening operations. To better understand how far we have come during the past two years, it is essential to recall how the pre-9/11 screening process worked and the safety disincentives that were created by a least-cost contracting dynamic.

Under the old system, private screening companies aggressively competed to secure contract awards from each airline carrier. Security was treated just like any other airline contractor commodity, with the winning bid usually being the lowest price. Since most of the security screening costs reside in labor expenses, these low-bid awards yielded a minimum wage work environment and atmosphere.

In addition, the selection of equipment used at checkpoints reflected budgetary caution rather than safety concerns. Passenger throughput needs often overrided sound safety decisions. Complicated by the airlines' financial responsibility, the government failed to sufficiently oversee checkpoint passenger screening, and the Federal Aviation Administration's ("FAA") training program lacked content and breadth. In short, the cross-purposes and financial incentives clearly tilted toward making checkpoint passenger screening just another line item to be constantly squeezed in an already financially-challenged industry.

As airline contractors in the pre-9/11 world, private screening companies assumed a broad array of responsibilities. These included worker recruitment, background checks, drug testing, and hiring; maintenance of all personnel files; and initial classroom, on-the-job, and recurrent training. Screening companies were contractually responsible to the airlines for any performance failures, which could include failing an FAA test or any other performance failure resulting in a breach of protocol, policy, or procedure. Failure to meet guideline standards in any area of responsibility could result in significant fines.

Of course, all of this changed after 9/11 with passage of the Act. While under contract to the government and during the interim twelve month period before complete federalization of airport screening, members of the current FirstLine management team were responsible for the operation of and ultimate transition to the TSA of checkpoint security screening at over 100 airports with over 12,000 screeners.

The Shift to the PP5 Program: FirstLine's Early Experience

On October 8, 2002, the TSA awarded FirstLine a PP5 program contract that initially called for 511 full-time employees to provide passenger screening at KCI. We were later informed that the original RFP failed to specify the personnel needs related to checked baggage screening. The new (continually adjusted) number grew to over 700 (presently, the employee counts has been "right sized" to 687).

In order to meet our personnel requirements, we recruited over 5,000 potential applicants through various recruitment methods. These included print and radio announcements (including placements with minority-oriented publications and stations), as well as the efforts of a professional recruitment firm, Job Plex. From this applicant pool, 3,494 candidates successfully completed our corporate pre-screen process, meaning that we might consider each individual for employment provided he or she successfully completed TSA's assessment and qualification process.

After our pre-screen, each candidate was referred to the TSA's "Quick Screen" application process conducted under contract by NCS Pearson. Of the original 3,494 candidates, 2,337 cleared the Quick Screen process and began "Phase I" of the TSA assessment process. Following Phase I assessment, this pool shrunk to 1,318 individuals who qualified for "Phase II" assessment.

At the end of this NCS Pearson process, 1,021 applicants were eligible for referral to TSA training conducted under contract by Lockheed Martin. From this assessment-qualified pool, we selected 647 of the original 5,000 applicants to be referred to Lockheed Martin for training. Only 582 of these candidates completed all required training and, accordingly, became eligible to be hired for screening positions.

It is important to note that, at no time did TSA, NCS Pearson, or Lockheed Martin permit PP5 contractor access to either the assessment or training process. To this day we do not know why certain individuals cleared or did not clear the assessment or training

procedures. We were specifically prohibited from shaping or gaining any insight into the parameters under which our soon-to-be employees had been qualified.

On November 19, 2002, just over a month after the contract award and only several days before the Thanksgiving holiday traffic, FirstLine assumed control for meeting the staffing requirements for checkpoint screening at KCI. In addition, despite the unexpected post-contract change in staffing requirements to accommodate checked baggage screening, I am also proud that our personnel fully met this additional mandate of December 31, 2002.

The Assessment and Training Process

The initial assessment and training process failed to produce the required number of qualified applicants. Recall that the number of required screeners had increased beyond the original 511 requested due to the baggage screening requirement added to the contract after the award date. However, once NCS Pearson, the TSA's assessment contractor, met the initial head count and/or time frame demands of its contract with TSA, it simply closed up shop and moved on to another location.

From the outset, because of this system breakdown, we never had the "required" number of trained screeners to meet the initial head count demand. Of equal importance, there existed no "ready pool" of applicants available to satisfy both anticipated and unanticipated employee attrition.

TSA's failure to provide ongoing or as-needed assessment and training, coupled with a mandated cross-training requirement that effectively took 50 screeners per week off the lines in advance of the busy summer travel season, resulted in an inability for FirstLine to replenish our screener ranks to meet the demand. On May 23, 2003, the Federal Security Director elected to bring in the Mobile Screening Force, a group of federal screening employees gleaned from excess staffing at several airports, to assist in filling the gap.

However, we were not permitted to do anything about this key staffing problem. Eight months lapsed -- from November 2002 to July 2003 -- during which time TSA's contractors did not make a repeat assessment and training process available to FirstLine. The inability to fill vacancies because of assessment and training process decisions severely frustrated our operations. Not until this past summer did we have the ability to recruit an additional pool of 1,763 applicants, of which 183 were certified, hired, and scheduled on the checkpoints, allowing for the Mobile Screening Force to be relieved of its responsibilities on July 29, 2003.

In short, FirstLine's ability to meet our obligations with the TSA at full staffing levels could not be realized because the assessment and training contractors were limited -- by their own contractual arrangements -- to the number of individuals that could be assessed and/or trained. Unfortunately, this continues to be an unresolved hurdle.

FirstLine's KCI PP5 Responsibilities and Challenges

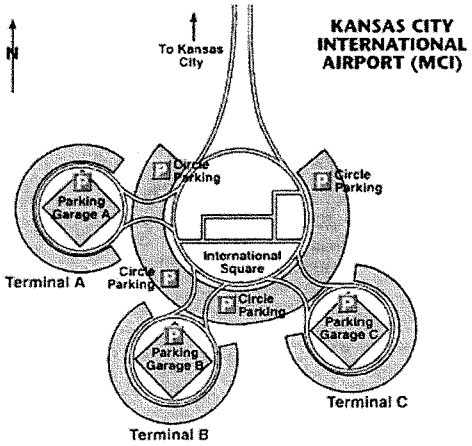
While it is difficult to overstate the impact that the assessment and training processes have had on our first year as a PP5 contractor, it is far easier to articulate FirstLine's responsibilities in relation to our TSA client and KCI's Federal Security Director.

Specifically, FirstLine is responsible for managing the screener workforce with respect to all human resource-related functions. This includes establishing pay and compensation schedules at or above the federal screener level; performing payroll-related activities; rewarding and disciplining for performance; hiring and firing; orchestrating shift bids; and scheduling (in concert with the TSA).

In addition, FirstLine is responsible for all other areas not directly related to security-related policy, procedure or process -- which fall entirely within the domain of the Federal Security Director and the TSA. We have neither input into scheduling requirements, nor do we interface with the airlines.

We are particularly proud of the work that our employees perform at KCI given the very unique facility issues presented by the airport's layout. For those of you who have not traveled to or through KCI, the airport is arranged in three horseshoe-shaped terminals, with the distance between a jetbridge entrance and the airport exterior entrance only a matter of a few dozen feet. It is possible to deplane and be outside meeting your ride within minutes.

This configuration requires 12 screening checkpoints and 9 baggage screening stations, exacerbating the need for balancing our workforce between checkpoints and baggage screening stations. In comparison, Hartsfield International Airport in Atlanta has 4 screening checkpoints.



Moreover, once a passenger clears security, another unique aspect of the airport layout that increases our employee's workload is the fact that access to restroom facilities, food and refreshments, and many other creature comfort or needs reside outside the secure area. Given passenger ingress and egress from the secure area, this creates the need to "double screen" many passengers.

Finally, to throw just one additional variable into the mix of our PP5 experience, KCI is presently undergoing a major remodeling. The work plan and construction progress result in both temporary and permanent gate relocations, which continuously require the reassignment of our screeners.

In the end, the TSA is our client, and despite the process and facility challenges that have been thrust upon FirstLine, our constant goal has been to ensure that our job is accomplished to the exacting standards required of every checkpoint and baggage screening operation around the Nation.

We welcome the open dialogue and close working relationship that we have been able to develop with Richard Curasi, KCI's Federal Security Director, to ensure that the security responsibilities for KCI are collaboratively met. Director Curasi's central focus on our shared security mission, and his personal efforts to foster a true partnership environment between his TSA and our FirstLine teams at KCI, are critical to the success of this evolving public-private screening model.

The Window of Opportunity

As FirstLine concludes the first year of our public-private partnership, and despite all of the challenges that we have faced as part of this TSA learning experiment, we are proud to be a key part of a passenger security that is no longer treated as an airline-driven commodity. This fact alone significantly enhances the mission at hand.

FirstLine fully supports TSA oversight and control of the safety and security of our Nation's airports. All private contractors must continue to be supervised and held accountable to high safety standards by the TSA. The inherent potential conflict between costs and safety that existed in the pre-9/11 model is now eliminated.

In our role as a PP5 program contractor, we continue to believe that our ability to bring private sector human services management enhances and improves the screening product that our employees deliver at KCI everyday. These factors include:

- Pay scales that can be determined by FirstLine, in excess of the government proscribed rates if market conditions require or warrant.

- Enhanced employee training to include customer service as well as security-related training.

- Rewards for exceptional performance and attendance.
- Employee involvement through our Employee Advisory Committee.
- An ability to discipline or offer corrective guidance in a timely manner.
- Management responsiveness to employee concerns in real time.
- Flexibility to tailor the structure of our effort to the unique demands of a facility's environment, such as those that exist at KCI.
- The overall ability to remove the ever increasing burden of day-to-day workforce management, allowing the federal government to focus on security, safety, and technology priorities.

At the same time, the PP5 program's final year offers Congress, the TSA, and airport operators the ability to more proactively evaluate the role of private screening contractors. Specific adjustments that FirstLine recommends for immediate incorporation into the PP5 test pilot, and that would in no way compromise the high security standards that must be uniformly maintained, include:

- Increased local decision making ability -- both at the FSD and contractor level -- regarding items such as local control and implementation of assessment and training, both of which are critical to maintaining staff levels and to controlling overtime.
- Local TSA and/or contractor ability to respond to passenger traffic requirements.
- Adoption of a process for peer-to-peer discussion of security challenges between the TSA and the contractor partners.
- Flexibility for the TSA and PP5 contractor to initiate test initiatives at the local level.
- Objective performance metrics regarding PP5 performance evaluation standards that are communicated by TSA to PP5 contractors in advance.
- Development of objective benchmarks for comparing the PP5 approach in meeting required mission standards to the overall federal screening program.
- Funding support for software management tools that enable maximum workforce utilization, as well as maintenance of employee performance and training records.

- A broader commitment to the public-private partnership in order to inculcate best practices and enhance cost efficiency without compromising the mission at hand. Contractors should be allowed to more appropriately leverage private sector strengths while government regulates and enforces safety standards and quality.

* * *

Mr. Chairman, our PP5 experience has convinced us that the private sector has much to offer TSA in our post-9/11 model and approach to passenger and baggage screening. With appropriate modifications to the PP5 program, these contributions could be even more easily identified and measured in the coming year.

On behalf of FirstLine and our employees, we are committed to ensuring that the second year of the PP5, and our work for the traveling public at KCI, continues to enhance the security of our airline passenger system. FirstLine is available to provide any additional information the Committee may request.

Mr. SHAYS. Mr. NcNeil.

Mr. MCNEIL. Mr. Chairman, McNeil Security, Inc., a subsidiary of NcNeil Technologies, is pleased to testify before the Committee on Government Reform.

McNeil Security has a contract with the Transportation Security Administration to provide security screening at Rochester International Airport in Rochester, NY. Rochester Airport is a category II airport and is one of the five designated pilot program airports. Although we were not involved in commercial airport screening prior to the establishment of the TSA, we have an extensive security screening expertise providing access control and related security services to a number of defense facilities.

All of our screeners employed at Rochester International were selected using the same process and requirements as those of airports with Federal screeners. The basic training program, provided by Lockheed-Martin and Boeing, was identical to the ones given to the Federal screening. The same on-the-job training requirements and testing procedures leading to certification were also used.

Staffing requirements, checkpoints and baggage screening operation procedures and reporting methods are the same for those at Federal airports. The daily operations are monitored by the TSA screening managers. Scheduling and other duties performed by TSA screening managers at Federal airports are accomplished by McNeil Security supervisors at Rochester.

McNeil supervisors are assigned additional duties to their TSA-mandated functions, such as training, supply procurement, scheduling, and so on. This has enhanced the development of our supervisors but also helped foster teamwork between TSA and McNeil Security. One example of this was the development by McNeil Security supervisors of a procedure and forms that accurately catalogs various data TSA requires on a daily basis.

Training is a serious issue for McNeil Security. It cannot be overstated that the training provided to one of the first lines of defense in aviation safety must keep pace with the resourcefulness of terrorists. This begins with basic training, where customer service and security are held on equal planes. While there is nothing wrong with encouraging screeners to be polite, respectful and friendly, speeding passengers through a checkpoint to avoid delays must never take priority over security.

It is a fact that while numerous wait-time surveys have been conducted, there has been little or no recurrent training provided except which McNeil Security has provided. Screening supervisors are given no additional training beyond the basic screening training course. Until very recently, no TSA-sponsored training for supervisors was available. Basic problem solving, communications and other standard supervisor training has not been offered. This is despite the fact that supervisors have a myriad of duties outlined in the TSA SOP. The duties referred to involve alarm resolution, explosive trace detection, x-ray image interpretation, and other security-related functions.

This is an area where training and interviewing techniques and the recognition of deception will improve operations.

The recurrent and enhanced training provided by McNeil Security, strongly supported by Commander Bassett, the Federal Secu-

rity Director at Rochester, is bridging some of the training gaps. He has approved a variety of training programs we have initiated for our screening force. These include hand-wanding techniques, screening persons with disabilities, exit lane procedures, report writing for supervisors, concealed weapons, improvised explosive detection devices, recognition of suspicious behavior, communications for supervisors, and Operation Eagle Eye, which is recognition of suspicious behavior, evaluation and preparation for supervisors, leadership skills, explosive trace detection refresher ETD. Those are all supplied by McNeil Security. Commander Bassett also recently authorized a member of his own staff to conduct IED recognition training at the checkpoints. There has been discussion of a TSA on-line training initiative. While on-line training can be helpful, role playing, actual demonstration and other hands-on training is much more effective.

We would welcome some guidance and training in this particular area. This test also points to the customer service versus security dilemma.

Recertification testing was performed in August. McNeil Security has repeatedly requested access to the scores. We are interested in feedback about which questions were missed or any x-ray images identified as threats or no threats. We have no information on how the tests were validated.

In addition, without the aforementioned information, a valuable training tool was lost. It is not possible to identify those areas where screeners may need additional training. Screeners were supposed to be ranked by their test performance. This is important information for corporate actual performance reviews. To date, this information has not been provided.

Thank you.

Mr. SHAYS. Thank you very much.

[The prepared statement of Mr. McNeil follows:]

McNeil Technologies
Corporate Headquarters
6564 Loisdale Court
Suite 800
Springfield, Virginia 22150

703.921.1600
703.921.2018 (fax)
Human Resources Department

www.mcneiltech.com

CONGRESS OF THE UNITED STATES
HOUSE OF REPRESENTATIVES

TESTIMONY BEFORE THE COMMITTEE ON GOVERNMENT REFORM
NOVEMBER 20, 2003

Mr. James McNeil, CEO
{Accompanied by Mr. Michael Broida, Site Manager, Rochester Airport}
McNeil Technologies, Inc. – McNeil Security, Inc.
6564 Loisdale Court
Springfield, Virginia 22150

McNeil Security, Incorporated a subsidiary of McNeil Technologies, Incorporated is pleased to testify before the Committee on Government Reform. McNeil Security has a contract with the Transportation Security Administration (TSA) to provide security-screening services at the Greater Rochester International Airport (ROC) in Rochester, New York. The Rochester Airport is a category II airport and one of the five designated "pilot-program" airports. Although we were not involved in commercial airport security screening prior to the establishment of the TSA, we have extensive security screening expertise providing access control and related security services to a number of Federal defense facilities.

All of our screeners employed at Rochester were selected using the same process and requirements as those of airports with federal screeners. The basic training, provided by Lockheed-Martin and Boeing, was identical to that given to federal screeners. The same on-the-job training requirements and testing processes leading to certification were also used.

Staffing requirements, checkpoint and baggage screening operating procedures and reporting methods are the same as for federal airports. The daily operations are monitored by TSA Screening Managers. Scheduling and other duties performed by Screening Managers at federal airports are accomplished by McNeil Security Supervisors at Rochester. McNeil supervisors are assigned duties in addition to their TSA mandated functions, such as, training, supply procurement, scheduling and so on. This has not only enhanced the development of our supervisors but also helped foster the teamwork between TSA and McNeil Security. One example of this was the development, by McNeil supervisors, of a procedure and form that accurately catalogs various data TSA requires on a daily basis.

Training is a serious issue for McNeil Security. It cannot be overstated that the training provided to one of the first lines of defense in aviation safety must keep pace with the resourcefulness of terrorists. This begins with basic training where customer service and

McNeil Technologies
Corporate Headquarters
6564 Loisdale Court
Suite 800
Springfield, Virginia 22150

703 921 1600
703 921 2018 (fax)
Human Resources Department

www.mcneiltech.com

security are held on equal planes. While there is nothing wrong with encouraging screeners to be polite, respectful and friendly, speeding passengers through a checkpoint to avoid delays must never take priority over security. It is a fact that while numerous "wait time" surveys have been conducted, there has been little or no recurrent training provided except that which McNeil Security has provided.

Screening supervisors are given no additional training beyond the basic screening course. Until very recently no TSA sponsored training for supervisors was available[1]. Basic problem solving, communications and other standard supervisory training have not been offered. This is despite the fact that supervisors have myriad duties outlined in the TSA SOP. The duties referred to involve alarm resolution (explosive trace detection (ETD), x-ray image interpretation and other security related functions. [redacted] This is an area where training in interviewing techniques and recognition of deception will improve operations.

The recurrent and enhanced training provided by McNeil Security and strongly supported by Commander David Bassett, the Federal Security Director (FSD) at Rochester, is bridging some of the training gaps. He has approved a variety of training programs we have initiated for our screening force. These included "hand wanding" techniques, screening persons with disabilities, exit lane procedures, report writing for supervisors, concealed weapons, improvised explosive device (IED) recognition, communications for supervisors, operation eagle eyes (recognition of suspicious behavior), evaluation preparation for supervisors, leadership skills, explosive trace detection refresher (ETD). Commander Bassett has also recently authorized members of his own staff to conduct IED recognition training at the checkpoints.

There has been discussion of a TSA "on-line" training initiative. While on-line training can be helpful, role-play, actual demonstration and other "hands on" training is much more effective. [redacted] We would welcome some guidance and training in this particular area. This test also points to the customer service versus security dilemma. [redacted]

[1] TSA is now offering a basic supervision course developed by the U.S. Department of Agriculture. To date it has not been offered to McNeil Security supervisors.

McNeil Technologies
Corporate Headquarters
6564 Loisdale Court
Suite 800
Springfield, Virginia 22150

703.921.1600
703.921.2018 (fax)
Human Resources Department

www.mcneiltech.com

Recertification testing was performed in August. McNeil Security has repeatedly requested access to the scores. We are interested in feedback about which questions were missed or any review of x-ray images incorrectly identified as "threat" or "no threat". We have no information on how the tests were validated. In addition, without the foregoing information, a valuable training tool was lost. It is not possible to identify those areas where screeners may need additional training. Screeners were supposed to be ranked by their test performance. This is important information for corporate annual performance reviews. To date this information has not been received.

Recommendations

We recognize and appreciate the monumental effort TSA has in managing overall airport security operations. Based on our experience as a pilot program contractor, there are several recommendations we wish to offer.

1) Basic training needs to be revised to include much more "hands-on" experience with artfully concealed weapons, simulated IED models and review of actual items found during actual screening operations. Basic interviewing techniques should be added to the curriculum. Customer service training should be revamped more along law enforcement models of professionalism, self-confidence and civility rather than the "have a nice flight" model of an airline ticket agent. This would help enhance the screeners' perception of his/her job as a serious security related profession.

2) Constant training needs to be recognized as an essential component of overall operation with appropriate time allocated to this area. Technology is not the panacea. While Threat Image Projection (TIP) is a resource it cannot be relied upon to be the only training method. Role-play and actual objects are much more effective.

3) Screener focus groups should be formed to make recommendations about procedure and training. McNeil Security formed focus groups to address issues related to passenger screening with positive results. First, it is the screeners who know how the operation runs on a daily basis and second, it is a way to enhance morale and foster team building. Both of those are essential to maintain an alert dedicated workforce.

4) The focus on security should not be diluted with other issues [redacted]

Mr. SHAYS. What I am going to do is ask our counsel, David Young, to begin the questions.

As I see this panel, we basically really have the private folks who are involved in four airports. Mr. DeMell, how many airports do you do?

Mr. DEMELL. We do just the Kansas City International Airport.

Mr. SHAYS. Before I go to Mr. Young, you said there were 12 separate entrance ways—I thought you said, Mr. DeMell?

Mr. DEMELL. There are 12 passenger screening checkpoints.

Mr. SHAYS. You are not counting two machines side by side?

Mr. DEMELL. No, sir.

Mr. SHAYS. That strikes me as quite significant.

Mr. DEMELL. Kansas City, and we have a diagram in our written presentation, has a very unique layout. Not only are there 12 checkpoints and eight baggage screening stations, once you get into a secured area or the gate area where you typically sit to wait for your flight, if you have to use the bathroom or would like a coke or cup of coffee, you have to go out of the secured area and come back and get screened again. There are no facilities inside of the secured area because of the size and configuration of that airport.

Mr. SHAYS. You have a pretty unusual site.

Mr. DEMELL. A very unusual site.

Mr. SHAYS. Is that typical of the other four sites? In other words, did we choose to give the private sector the five hardest sites, or does this just tend to be the only one like this?

Mr. DEMELL. Kansas City International is unique. The only airport that may compare in some way would be LaGuardia. It is a larger airport with some similar challenges. Kansas City is a unique setup. There isn't another one like it that I am aware of.

Mr. SHAYS. OK. Ms. Berrick, let me ask you this. Were they chosen at random?

Ms. BERRICK. TSA's methodology for selecting the five pilot airports was to select one in each of the airport categories. So there is a category of the airports that are the largest and most at risk, down through category 4.

Mr. SHAYS. That would appear to make sense, correct?

Ms. BERRICK. We didn't look specifically at their methodology for selecting the pilots, but that seems to be a reasonable approach.

Mr. SHAYS. I will jump in after—maybe jump in while—my privilege—Mr. Young asks some questions.

Ms. Berrick, I will be wanting to ask you some questions other than the private sector play in this issue. I will want to know in general your assessments of port security and cargo and so on.

Mr. YOUNG. Thank you, Mr. Chairman.

I know that you have all spoken in your testimony about the need for flexibility with regard to the particular needs at particular airports. The Federal Security Director is supposed to be the focal point as the representative from TSA that is there to manage the security issues for particular airports. Understandably, there are standards that need to be met. There are requirements, regulations and laws that obviously need to be applied.

I am curious to hear from McNeil Security and FirstLine Transportation Security about your relationship with your Federal Security Directors, how you are interacting with those directors in im-

plementing TSA requirements and also how difficult or easy is it to do extra things. Like, Mr. NcNeil, you mentioned the additional training you have done, and, Mr. DeMell, I know you have also done additional training at your airports. So I am curious to hear what your experience is in having localized additional either screening requirements in terms of actual actions or practices that you all take and also additional training that you do.

Mr. DEMELL. I guess I can start.

In addition to the training that we have heard about that is mandated via the TSA, in Kansas City we recently instituted a program where every screener receives 3 hours of additional training every single week. Now that is an initiative that was put in place in conjunction with our Federal Security Director that was not a TSA Washington-dictated action. Screener supervisor training, we really have been given the latitude to do the things we think we need to do to make our supervisors better supervisors.

I will say, in the program as it is designed today, the relationship between the private contractor and the Federal Security Director is key. The program, in my view, was a bit of an orphan program for several months and the FSDs were really left out there with little direction and little help from Washington in managing this program. I think it has just been in recent months, the last 4 or 5 months, where things have begun to change, and I think we now are in the process of developing and have come a long way toward developing a true partnership in meeting the mission at hand.

Mr. MCNEIL. We are very fortunate at McNeil Security in Rochester to have a very good relationship with our Federal Security Director. He has allowed us to establish new training programs for our people that weren't originally prepared by TSA. We have, I guess, instituted about four or five different training programs for our people, including customer service, as well as explosive trace detection that were not originally offered. We also brought in some of the local police officers to give us specific types of training on identifying explosives as well as local military units to help us identify different kinds of weaknesses we might have.

Some of the problems that we are actually encountering, even though when we go to our Federal Security Director, there are some times when he has to go up the line to get information and get approval, and it is very difficult in fact for him to get approval for us to do certain things. For example, on recurrent testing, when we get people who have been tested, we continue to get the results of the testing on our own people to allow us to identify weaknesses in the test so we might be able to design a training program to strengthen the areas in terms of where they fail the tests. We are still trying to get information in that regard. All in all, I think it has been a very good relationship, but a very difficult one from the standpoint of actually trying to get information from headquarters.

Mr. YOUNG. With your experiences with doing these extra training activities, does TSA seek input from you all in terms of ways to improve their own programs so that, if some of the programs you are doing might be beneficial to TSA as a whole, is there a mechanism for you to be able to transmit that information to TSA?

Mr. DEMELL. There is a mechanism that flows through the local Federal Security Director as it relates to FirstLine's experience,

and we also are very involved with ideas from the screener level up. We have an Employee Advisory Council that meets bimonthly—I am sorry, twice a month—and part of their responsibility is to offer suggestions for improving the security function in Kansas City International Airport.

Mr. MCNEIL. The same has been true with McNeil Security. We do also have ways of getting information up through the system and getting approval. We also have an Employee Advisory Council that provides feedback from the employees in terms of morale and other things we can actually do to promote that.

The biggest difficulty I think we have is that the pilot programs have been sort of ignored. No real attention has been paid to them. I think most of the focus has been on the other airports, opposed to saying this is separate and distinct and how can we treat them that way.

Mr. YOUNG. So you believe then that, although you are sending up information, that TSA isn't taking the information as seriously as they are taking it from other airports?

Mr. MCNEIL. In my opinion, if it is not part of the basic training or the basic kinds of things they are doing for all airports, then they don't really take it very seriously.

Mr. YOUNG. Thank you.

Ms. Berrick, I know we have again talked about flexibility. On the other hand, though, we do need to make sure there is standardization because there are passengers that need to go from airport to airport. They have to be familiar with the different standards as well as airlines that have to deal with the various rules. Has GAO thought of what the balance needs to be or made any suggestions with regard to flexibilities with that in mind?

Ms. BERRICK. We are currently looking at the issue you just mentioned in terms of what is the appropriate balance, and we are going to be issuing a report on that subject in April. I can tell you, based on the work we have done, obviously the authorizing statute for the five pilot airports identified that the standards have to be comparable, at least at a minimum with the standards that TSA has in place, and pay and benefits have to be comparable but we believe even within that makeup there is room for some flexibility that TSA could afford the five pilot airports to determine whether or not they could achieve some efficiencies. As a part of—we issued a preliminary report on this subject in September, and we did mention that we heard some concern from some of the pilot airports that they weren't given some of the flexibility they wanted in terms of doing additional training, in terms of having additional testing at their airports, and we are looking into those areas further as a part of this review.

Mr. YOUNG. It sounds like from our folks here that might be improving a little bit in terms of their relationship with the FSDs.

Ms. Berrick, coming back to you and moving a little bit toward supervisor training, I know that you had mentioned that GAO had some recommendations in terms of what TSA might be looking at in terms of supervisor training in addition or perhaps different from their current use of the USDA graduate school basic manager course. Could you comment a little bit on that?

Ms. BERRICK. My first comment, again, is that we are continuing to look at training as well so we will have some additional information on this later. But the initial concern that we had in looking at this area was that supervisors were telling us there was no supervisory training and they really needed that training in order to do their jobs. Also TSA's Internal Affairs Office that does covert testing at the screening checkpoints cited supervisory oversight as a problem causing some of these screener testing failures. So we think it is very important.

TSA has since taken some action to help correct that. They are taking a USDA graduate school course, a general supervisory course that they started giving some TSA screening supervisors, and they are going to modify that course to meet the specific needs of the screening supervisors. We think that is definitely a step in the right direction. Still, the immediate problem is that has to be going out to all supervisors within TSA. I think TSA reported that 500 supervisors have gotten that training system. However, we believe it needs to go out on a widespread basis to make sure everybody gets that training. Then we are looking at what will be some additional training that will be useful for supervisors.

Mr. YOUNG. Thank you.

For FirstLine Transportation Security and McNeil Security, what kinds of training do you think are necessary for your screener supervisors?

Mr. DEMELL. I think they need the basic HR training that every supervisor needs to develop the skills to manage people. I might also add, in reflecting on Mr. McHale's testimony, the TSA has two sets of problems. One-half of their plate is filled with managing the work force, and I really think that is what companies like FirstLine bring to the table. By enabling us to handle all of the HR functions, the supervisor training, the ongoing training, removing all of the HR issues from the TSA's plate, we allow them to focus on process, procedure and technology. I think that marriage of those two efforts brings the completion of the mission at hand to a much better conclusion in a positive way than the processes that are in place today.

Mr. YOUNG. Mr. NcNeil or Mr. Broida.

Mr. BROIDA. I will address that.

The supervisory training which TSA has not provided, there are two important parts. What Mr. DeMell said is certainly true. But, in addition, the SOP refers to many, many specific duties of a supervisor in alarm resolution, for example. In those cases, neither the SOP nor the training gives any guidance to the supervisor of actually how to perform those functions. In fact, I myself am a certified screener; and when I went through the school I asked the question of the instructor who said, "Well, it says notify your supervisor. I am the supervisor. What do I do?" The instructor said, "That is it." You are the supervisor, and no guidance was given. That has never been clarified since, and that was—I graduated from screener school on November 15, 2002.

So our supervisors were sort of given only a half training, and that has never been filled in. While the HR issues and basic supervisor skills are indeed important and we at NcNeil have provided some of those courses—we gave a training course, an active listen-

ing course for our own supervisors—these types of things in dealing with alarm resolution and the actual supervisory duties of overseeing a security checkpoint are completely lacking.

Mr. YOUNG. Thank you.

I also know from some of the information, Mr. NcNeil, that you spoke about some of your additional training with regard to interview skills and those kinds of things. How helpful do you think that is for screeners in terms of being able to not only just be able to operate the machines but also to be able to observe people and how they react to situations? I am just wondering if you all have any examples of how that might have been used or was helpful in a particular situation.

Mr. MCNEIL. Mr. Broida is going to answer that.

Mr. BROIDA. Earlier when Mr. McHale was testifying there were questions about weapons that had been found and how people say, "Oh, I just forgot it," and things like that. We were rather incredulous—and I have been actually on the job—with the number of weapons people bring to secured areas and say they just forgot about. Recently—well, in the course of our experience at Rochester, there are two incidents in which handguns were detected by our screeners at checkpoints. In both of those instances, they were legally registered handguns and the persons with them had pistol permits, New York State carry permits, and their explanation was they simply had forgotten they were in their various pieces of luggage.

However, the supervisor is the first person there and has to begin asking questions. Do you know what is in your bag? Why is it in your bag? Questions like this. Without any training and interviewing techniques or the ability to detect deceptive responses, our supervisors really do not have the ability to begin that type of an investigation.

I think that basic interviewing techniques are of extreme importance to all screening personnel. In Rochester, our checked baggage system right now is an ETD system in the lobby, a post-check-in system. Therefore, the passenger is present when his baggage is screened. It is not uncommon to have ETD alarms which can be caused by things other than explosives. I can't comment on those things, obviously. But one of the things that is done when such an alarm takes place is a resolution in which the supervisor is supposed to ask—or the screener—a series of questions without any training in how to ask those questions and detect if the responses are deceptive.

Mr. YOUNG. Thanks, Mr. Broida.

Just kind of to wrap up, Ms. Berrick, today the TSA, Mr. McHale, spoke about the short-term screening improvement plan that they have in terms of the things that they are going to be working on and their priorities in terms of improving passenger screener training, testing, supervising, all those kinds of things. Does GAO have some kind of comment about TSA's approach in terms of taking an immense problem that has existed even before TSA even existed and given the fact that there have been limited time periods that Congress has given TSA to handle and hire lots of people and make sure they are ready? Can you just comment a little bit about their approach in terms of looking at the problem,

trying to analyze it, and look at a road map for solving those issues?

Ms. BERRICK. Sure. We think we included this in our testimony in some prior work that GAO did.

The first thing TSA really needs to focus in on is measuring how well their passenger screening program is performing, and that starts with establishing metrics from which to measure and then determine whether or not they are improving as they make all these enhancements to their passenger screening program. One way to do that is through increasing their testing program. That is a great way to get data on how well they are performing, and TSA does have some plans to do that. Another way to get additional performance data is to put the TIP system, the Threat Image Protection system, nationwide so you can collect a lot of additional performance data that you are not going to be able to get through screening. The annual screener certification program is another way to get performance data on how well screeners are performing. We think TSA needs to continue strengthening their efforts to determine how well they are performing and, based on that information, determine where they need to focus their resources.

We think that the screener improvement program that they went through was a great idea. We are looking at that right now to see if they are developing action plans and how exactly they plan to followup on the issues that they identified. But, again, we think the focus should be on measuring their performance and from there determining where their weaknesses are.

Mr. SHAYS. Thank you, Mr. Young.

Let me just ask the private sector here, give me the bottom line as to what you think the issue is right now as we approach the time in which airports can opt out of the public sector and choose private sector.

Mr. DEMELL. I think the real challenge is differentiating the private contribution from the public-private contribution. Because there has been little latitude and little flexibility built into the system, we struggle to differentiate ourselves. I think, as I stated earlier, that our contribution on the HR side to the management of the work force has to be a prime consideration in looking at the public-private partnership as viable going forward. I think that is where we bring a lot of tools to the table that possibly the Federal Government is not able to bring or is not able to bring at the level that we are.

Mr. SHAYS. Thank you. I would like both of you to respond.

Mr. MCNEIL. I would agree with Mr. DeMell from the standpoint that if we were to allow more flexibility in terms of staffing the jobs, in terms of determining what are the staffing requirements that we have—because in some cases we believe we could staff it with less people than required by TSA to do the job. A little more flexibility in terms of being creative, being innovative in some of the solutions that we have.

We formed several focus groups in the organization, both on the baggage as well as its passenger side, to identify ways we can actually be more efficient in terms of how we do our jobs. If we were able to have a little more flexibility in implementing some of those—and then again, training, if we could be just a little more

flexible in terms of the training we have offered. Most of the training we have offered has added very little additional cost to our budget. We have sort of eaten that in-house. But getting from local law enforcement agencies that has the training professionals on staff, they are eager to actually provide that training for us.

Mr. SHAYS. What I understand when you are talking about flexibility, it is that you can train them to do anything, as long as you are willing to pay the cost, correct?

Mr. MCNEIL. That is not correct. We have to get approval before we can do any type of training, whether there are costs incurred or not.

Mr. SHAYS. I would think once you did the training you were required to do that you have met the test, and then any additional training you still have to get approval?

Mr. MCNEIL. That is correct, sir.

Mr. SHAYS. When you seek to get that approval, do you get it?

Mr. MCNEIL. Not always. In some cases it takes a very long time for it to go up the chain and come back, and in some cases it is denied. In some cases our Federal Security Director has just said, "I am just going to do it. I don't care what they say. It is easy, it is reasonable, it makes sense. Let's do this."

Mr. SHAYS. Do I pronounce your name Broida? Did I mispronounce it when I first——

Mr. BROIDA. It is Broida, sir.

Mr. SHAYS. I apologize.

Mr. BROIDA. Yes, what Mr. NcNeil said is certainly true. There was a directive from TSA headquarters—I am sorry I don't have it with me and I can't quote the date—but it addressed the issue of private contractors offering screening outside that which is offered by TSA. In sum and substance, it basically said we could provide training that was non-security-related any time we wished and they had no interest in that. However, anything that approached security issues or SOP issues had to be approved by TSA headquarters by going through the FSD.

In those cases, for example, the IED training involving the local law enforcement agency which we instituted. I brought that to Commander Bassett, and he approved it on the local level and then sent it up for upper TSA approval. I don't know whether or not he ever received the official sanction, but, fortunately, the Commander said, "You know, it is important training, let's just do it." It is a police agency. What is wrong with that? We certainly appreciated that.

Mr. SHAYS. Thank you.

Ms. Berrick, it would strike me that they would set up general task objectives for the private sector to meet and the public sector, and it would strike me that you would then—if they wanted to feel comfortable that there was basic training, they would say you have to do all of the above. Tell me what the logic is for—and I know I probably should have asked the previous panel this, but what is the logic for needing that approval to teach in addition?

Ms. BERRICK. That probably will be a good question for TSA, but just giving my opinion——

Mr. SHAYS. Not would be; it would have been.

Ms. BERRICK. It would have been, correct.

Giving my opinion, I think TSA has mentioned in the past that when you look at the authorizing statute for the pilot program airports, there is some restriction in that statute basically saying it has to meet, at a minimum, TSA standards and also the pay and benefits have to be comparable. I think they are interpreting that to the strict letter of the law. But I believe that, even the way the statute is written, there is some flexibility that could be afforded the pilot airports in these areas. One of them is what you just mentioned in terms of having minimal standards and let the pilots determine how they are going to achieve those, with TSA's oversight. That could be one way to do it, instead of saying all pilot airports have to adhere to this specific program and you can't go beyond that.

Mr. SHAYS. There are only five airports we are talking about, correct?

Ms. BERRICK. Correct.

Mr. SHAYS. So it seems to me they could send a supervisor, and if they objected to what was happening, they could note that for the record.

What I would suggest for our staff is that we consider writing a letter to—and I would like to think there is someone from TSA here now—stating that we think we need—obviously, the chairman would have to concur—I am struck by the fact that there needs to be a little more flexibility to ultimately assess the value of the private sector's participation. So I think we will do that. Do you think that would be helpful?

Mr. DEMELL. It would be very helpful. It is a frustration that is shared not only on the private contractor side but by our individual FSDs.

Mr. SHAYS. In other words, that even within airports done by TSA that they should be allowed a little bit more flexibility?

Mr. DEMELL. In a lot of these areas, yes.

Mr. SHAYS. For instance, if LaGuardia wants to do something above and beyond, they should be able to do that?

Mr. DEMELL. That is what I am saying.

Mr. SHAYS. Nodding the head doesn't get us on the record.

Mr. DEMELL. What I am really saying is our FSD—I can only speak for the Kansas City Airport. When I say our FSD is frustrated by some of the restrictions as we are, the private contractor.

Mr. SHAYS. Let me put it in my language. The airport is as frustrated as you are that you aren't given the flexibility.

Mr. DEMELL. Correct.

Mr. SHAYS. What I am wondering, possibly even give a little more flexibility within the public sector, if the folks at LaGuardia feel they would like to see a little higher standard or a little more flexibility or whatever, would they have the capability to see a little bit of—not uniformity—in other words, I am thinking intuitively that we want a uniform—we want a minimum standard of capability, but if we have even within the public sector a desire for an airport to go above and beyond, do they have that capability and shouldn't they have?

Mr. DEMELL. I think, Mr. Chairman, that was one of the ideas behind the public-private partnership, and that was something that

this partnership should have been able to design and implement and put into place to be looked at by the rest of the system.

Mr. SHAYS. OK. We know we have our work cut out here. It seems to me we are not taking advantage of what we wanted to have happen.

Just before we break, Ms. Berrick, I want to ask you, as it relates to air cargo—first off, let me understand, in your capacity in GAO you oversee Justice and—what aspect of Justice do you oversee?

Ms. BERRICK. I am about one of five directors in Homeland Security in the Justice team, and I oversee all transportation security work, including all the aviation work. So that would include air cargo.

Mr. SHAYS. And what over in Justice do you oversee?

Ms. BERRICK. My primary focus is aviation and transportation security. I do some court and jail work within the Justice side.

Mr. SHAYS. Talk to me about air cargo. I look at this sheet here, the aviation rings of security, and I gather that when they talk about airport perimeter and terminal that somehow that must include employees that work within the airport but I don't see it specifically mentioned. When I see 100 percent baggage check, it is like there should be an exclamation point, yet I realize that 20 percent of what is in the belly of an aircraft is not checked, and that is cargo because cargo represents about 20 to 21 percent of what is in the belly of an aircraft. Is that correct?

Ms. BERRICK. That is correct.

Mr. SHAYS. So help me understand why I should feel comforted that 20 percent of the cargo in an airplane—20 percent of what is in the belly of an aircraft—is not checked. Why should I feel comfortable about that?

Ms. BERRICK. The security of air cargo is a vulnerability. There is no question about that.

TSA, the way they are approaching that right now is through the known-shipper program which we talked about a little bit earlier. They are doing targeted inspections of air cargo. They are also investing, I believe, $55 million for 2004 in R&D looking at air cargo.

But, having said all of that, still 10 percent of air cargo is not screened, and that is a vulnerability. Given the fact that air cargo is on commercial aircraft with traveling passengers, that just heightens the concern. But, I agree, it is a vulnerability that needs to be addressed.

Mr. SHAYS. When we dealt with the vulnerabilities of baggage not being checked, we put a deadline on it. What is the negative of our putting a deadline on cargo screening for passenger planes?

Ms. BERRICK. I think the negative side of that is TSA not having the means with which to meet the deadline in terms of having the technology in place to do that.

Mr. SHAYS. But my understanding is that the luggage—excuse me, the cargo on the passenger plane somewhat conforms to what is the cargo—what is the baggage. In other words, it is at least smaller containers, isn't that correct?

Ms. BERRICK. I think it is of varying sizes. We are not specifically looking at the air cargo issue right now. We have done some work in the past. But my understanding is it is varying sizes.

Mr. SHAYS. Guess what? We are going to ask you to do that.

Ms. BERRICK. I will be happy to.

Mr. SHAYS. You can't come and testify here that it is a vulnerability and then—I realize you have, but it is something—I know the chairman is concerned about it.

Ms. BERRICK. As I mentioned, GAO did do some work looking at air cargo security about 8 months ago. It is somewhat dated, but we did identify air cargo as a vulnerability.

Mr. SHAYS. Tell me why I should feel comfortable about what we are doing to guarantee—"guarantee" is a bad word, we can't guarantee—but to help protect the traveling public by what we do to ascertain the—let me back up. What do we need to do to better protect the security of an airplane based on those who work on those aircraft and those that move within the airport, the employees?

Ms. BERRICK. One way to do that is through strengthening background investigations for airport workers, which was done after the Aviation and Transportation Security Act was passed.

Another effort is to focus——

Mr. SHAYS. I am asking an unfair question right now. Let me first ask it in a way that I think is fair to you. What studies have you done—what studies has GAO done to look at security in airports as it relates to the area of the airport and the employees who work within it?

Ms. BERRICK. We have two ongoing studies right now that haven't been completed. They should be completed in the March-April timeframe. One is looking at perimeter security and access control, and specifically we are looking at requirements that were spelled out in the Aviation and Transportation Security Act and whether or not TSA has complied with those requirements. We also have a review looking at the MANPADS threats, including what the Department of Homeland Security and TSA is doing to protect aircraft from MANPADS and what are some countermeasures that could likely be used to protect the aircraft. So, in answer to your question, we have two ongoing reviews that haven't yet been completed in that area.

Mr. SHAYS. Now if you wanted to answer anything more on the first question I asked, any recommendations of what needs to be done?

Ms. BERRICK. At this point, no, since the review is still ongoing, but I believe we will when it is completed.

Mr. SHAYS. It will be done by when?

Ms. BERRICK. April 2004.

Mr. SHAYS. Let me just ask Mr. DeMell and Mr. NcNeil, you are working at two airports, but you must wonder sometimes as to the security not related to passengers, the security of the people who work there. Do you have a sense and can you make a contribution to the discussion as to how secure our airports are in terms of our employees and so on? Do you believe that we need to make progress there and, if so, do you think we have vulnerabilities in any particular area?

Mr. DEMELL. I think we do need to make progress as it relates to both cargo and workers who have access.

Mr. SHAYS. I guess what I am wondering is, as you seek to make sure that the passengers that get on the plane don't present a threat, do you sometimes wonder if the employees that work at the airport have to go through the same kind of screening and do you sometimes question if we may be more vulnerable there? That is really what I am asking. If the answer is yes, have you thought about what we need to do to correct it? First off, I want to know if the answer is yes or no.

Mr. MCNEIL. The answer for McNeil Security at Rochester International is the airport workers go through basically the same type of background investigation that our people go through in terms of having their fingerprints through the FBI and the rest. What really concerns us, though, is, as we check baggage that goes on board the plane, someone that comes up to the counter, drops off a small package, that same package has no screening whatsoever, goes on board the plane. That is what really concerns us a lot of the time.

Mr. SHAYS. Tell me how that happens? That is not cargo. Is it called cargo?

Mr. BROIDA. Yes, sir. It is actually defined as cargo. Several airlines have programs where, if you need to get something to a certain place and it can't be Fed-exed in time, you can bring it to an airport and it will be put on a scheduled airliner to be taken to whatever that city is. That is considered cargo and is not subject to screening.

As a matter of fact, this came to the fore in Rochester when a NcNeil screener saw this occurring and thought that was rather bizarre and asked if he could screen it anyway. He volunteered to EDT screen it and was told he could not do because that was not in the TSA SOP.

Mr. SHAYS. Let me get this straight. The passenger who goes onto an airplane has to go through your system and their baggage is checked. You are saying it is conceivable in some airports that someone can come up to the front desk and present a package as cargo and not only is it not screened, that when you wanted to screen it you were not allowed to screen it because it was perceived as not being the luggage of a passenger, therefore not your responsibility and therefore you did not have the right to look at it? Is that what you are saying?

Mr. BROIDA. Yes, sir, that is correct.

Mr. SHAYS. Have you encountered anything as bizarre as that?

Mr. DEMELL. I have not.

Mr. SHAYS. Are you aware this may be happening?

Mr. DEMELL. Yes, I am.

Mr. SHAYS. That literally someone can come to the airport and drop off something as cargo and that it will be put on an aircraft and may be not screened?

Mr. DEMELL. As cargo or mail.

Mr. SHAYS. Cargo or mail, and it will not be screened?

Mr. DEMELL. Correct.

Mr. SHAYS. So you have never asked to have it screened, so you never had that experience. But you know as a fact it is put on the plane unscreened?

Mr. DEMELL. That is correct.

Chairman TOM DAVIS. Mr. Chairman, it is great to get that on national television and on the record.

Mr. SHAYS. Mr. Chairman, you have the floor.

Chairman TOM DAVIS. Ms. Berrick, I know you have said you have limited information on screener performance, but based on the work that you have done do you have reason to believe the current screeners are better, worse, or about the same as before September 11?

Ms. BERRICK. We really can't make that conclusion based on the information that exists. GAO did look at the passenger screening program prior to September 11 when the responsibility fell under FAA, and we are currently looking at it right now. What we are doing is looking at how TSA measures the performance of its passenger screeners, and we are finding there is really limited data out there that identifies how well their screeners are performing. As a result, it is very difficult to make any kind of comparison.

Surfacely, it looks like there have been lots of improvements: The pay and benefits are better, there is less turnover, etc. But in terms of concrete data on whether or not they are detecting harder-to-spot threat objects, we haven't seen that.

Chairman TOM DAVIS. Does GAO have an opinion on the current staffing levels?

Ms. BERRICK. We have an ongoing review that is looking at staffing levels. We reported in September of this year that, based on our preliminary assessments, some Federal Security Directors did express concerns about staffing levels at their airports in terms of having input into the staffing process. We are encouraged that TSA has recently hired a contractor to come in and assess their staffing model to get a second set of eyes looking at it. But staffing is a big concern based on the Federal Security Director we spoke with, and we are going to continue to look at this as part of our review.

Chairman TOM DAVIS. Let me ask the private companies. Mr. DeMell, are there any recommendations you would make to TSA regarding staffing levels that could create cost savings without jeopardizing security?

Mr. DEMELL. Since we haven't been able to participate in that process it is difficult, but we think that is an area where the private contractor should be allowed to interact with the local TSA in developing those staffing standards—not only staffing standards but looking at the organizational charts of the local TSA organization versus the private contractor, looking for overlap in ways to save money where there is a duplication of that effort in that end of it as well.

Chairman TOM DAVIS. Let me go back to Ms. Berrick. As a general rule, are airports able to fully staff their airport screener requirements?

Ms. BERRICK. Not always. There are peaks and valleys we found in terms of the Federal Security Directors not having the staff they need to respond to those peaks and valleys. One of the big things initially that the Federal Security Directors told us was they would love to hire part-time screeners. Recently, TSA has enabled the airports to do that, and that has been a big help. But there still is a problem in staffing, hiring the part-time screeners and making

sure that the airports have what they need when they need them, and we are continuing to look at that.

Chairman TOM DAVIS. OK. Let me ask, what about the TSA mobile units? How are those working out?

Ms. BERRICK. I don't have a lot of specific information on that. I believe one is deployed to Kansas, one of the PP5 airports, because there was a shortage there; and I don't have much more information on that, other than I know they are in use.

Chairman TOM DAVIS. OK. Thank you.

Mr. SHAYS. Let me close this hearing by just asking, is there anything that any of the four of you would like to put on the record, anything that you had maybe spent the night thinking about that we didn't ask you that needs to be part of the record?

Ms. BERRICK. If I could make just one comment, we are talking a lot about the five pilot airports. TSA recently hired a contractor to assess the performance of the five pilot airports. We think it is going to be challenging for that contractor to do an assessment because of the lack of performance data not only at the five pilot airports but throughout all the commercial airports in terms of how well the screeners are performing. So that is one thing that we are going to be working with TSA in looking at in terms of how this contractor is going to be able to assess the performance. Not only because there is a lack of data but also because the five pilot airports haven't been granted a lot of flexibility. So to do a true assessment I think will be a challenge for them.

Mr. SHAYS. I am struck by the fact, though, wouldn't it have been great if the TSA had allowed for innovation and not one-size-fits-all at all the airports so we could even compare within the public sector what might work better? Then obviously we would have allowed for the private sector to have the freedom to do a lot more things and to be corrective. That was the whole point, so we could then do an evaluation. It strikes me it is almost a study designed to fail because of that based on what you are pointing out.

Mr. Chairman, are we all set?

Let me again thank all the witnesses and say that this hearing is adjourned.

[Whereupon, at 1:35 p.m., the committee was adjourned.]

[The prepared statements of Hon. Dan Burton, Hon. Henry A. Waxman, Hon. Elijah E. Cummings, and additional information submitted for the hearing record follows:]

Statement of Congressman Dan Burton
Government Reform Hearing
November 20, 2003
"Knives, Box Cutters, and Bleach: A Review of Passenger Screening Training, Testing and Supervision"

Thank you, Mr. Chairman. And, as we embark on the busiest travel season of the year, thank you for holding this hearing. This is a very timely subject as we all prepared to visit our families for the holidays.

Two days ago, I met with members the Coalition of American-Owned Security Companies. The Coalition of American-Owned Security Companies consists of large, active and experienced American-owned private security companies in the United States. Coalition members include Barton Protective Services, Inc, Command Security Corporation, WSA Group, Inc. and GateSafe. Combined, these American-owned private security companies have over a half-century of experience providing a vast array of security services for many governmental entities and industries, including a wide variety of airport services.

When the Aviation Transportation Security Act (ATSA) was passed in 2001, Congress mandated that the responsibility for passenger and baggage screening would move from airlines to the Federal government. By November 19, 2002, Transportation Security Administration (TSA) screeners were in place at each of the 429 commercial-service airports in the United States.

Under ATSA, airports will be able to start applying to have screening services performed by private security companies under contract with TSA beginning in November of 2004. ATSA also requires that such private security companies be owned and controlled by U.S. citizens to the extent that such companies exist. This provision presents the TSA, airports, and private security companies with an exceptional opportunity to create a meaningful program that will incorporate the best practices and experiences of TSA, airports and the private security industry.

Mr. Chairman, there is an active and experienced American-owned airport security industry in the United States that is ready to meet today's security challenges. Private security companies have experience in every major airport in the country and have held contracts with every major airline. The industry has employed, recruited, and trained thousands of screening staff, and helped millions of passengers through security checkpoints throughout the United States.

As a part of the wider airport community, many American-owned private security companies also provide other airport services for airlines or airport clients. These range from security services—such as food and catering security, access control and perimeter patrol—to passenger services—such as skycaps, baggage handling, ticket verification and wheelchair assistance. Additionally, security companies provide security officers, access control and security consulting services to a multitude of industries beyond aviation.

In the new security environment that has emerged since the terrorist events of 9/11, the private security industry has undergone significant change. During my meeting with the Coalition, I was

informed that the industry welcomed greater Federal oversight following ATSA, and has embraced the movement toward the implementation of common professional standards for the security industry. Private security companies have the capacity, expertise and willingness to continue to serve in the airport security environment.

In 2002, TSA faced significant challenges in recruiting, training and mobilizing tens of thousands of screeners. Current budget and staff constraints continue to underscore the difficulty of running a uniform system across hundreds of different airports, each with its own challenges. In this environment, the private sector can provide an additional resource for the government—for example, in staffing, customer service, security, operational efficiency and aviation industry experience.

ATSA provides airports with the opportunity to apply to opt-out of Federal security provisions beginning in November of 2004. This presents the TSA, airports, and private security companies with an opportunity to create a meaningful partnership program that would incorporate the best practices and experiences of TSA, airports, and the private security industry.

In defining the program, the input of both airports and the private sector is essential. With only one year before the opt-out process commences, TSA, airports and private security firms must move quickly to ensure that this program is implemented effectively and meets the needs of the public and the aviation community.

A public-private partnership incorporating TSA, security companies and airports would bring mutual benefits and would facilitate effective resource management in the provision of safety and security to the public. The industry has both the experience and capacity to turn this public-private sector collaboration into a successful partnership that can be replicated across other industries. I sincerely hope that the TSA coordinates with the private sector and the airport community as the opt-out process commences. Thank you again for convening this important hearing, Mr. Chairman.

Statement of Rep. Henry A. Waxman, Ranking Minority Member
Committee on Government Reform
Hearing on
"Knives, Box Cutters, and Bleach:
A Review of Passenger Training, Testing, and Supervision"

November 20, 2003

I welcome this hearing on the importance of effective training and supervision of airport passenger screeners. As the attacks of September 11 made abundantly clear, screeners are essential to our entire system of aviation security. During consideration of the Homeland Security Act, I strongly supported creation of a federal workforce of security screeners. Now that we have one, we need to make sure they have high quality training and effective supervision.

Mr. McHale, one our witnesses today, says that in the 20 months since its creation, TSA has greatly improved aviation security, including passenger screening. This is an encouraging report. But as the recent incident involving Nat Heatwole illustrates, TSA still has a long way to go. Mr. Heatwole is a college student who managed repeatedly to sneak

dangerous items past security screeners. These included box cutters, clay that simulated plastic explosive, and liquid bleach. On two occasions, he concealed these items in airplane lavatories for extended periods of time.

This does not inspire a great deal of confidence. It also does not inspire confidence that it took TSA's commercially-run public complaint center five weeks to notice explicit e-mail messages from Mr. Heatwole explaining exactly what he did.

Two recent reports – one from the Department of Homeland Security's Inspector General and the other from GAO – raise additional concerns about the private contractors who prepare training materials and TSA's program management. The Inspector General concluded that TSA's training protocols maximized the likelihood that students would pass. After reviewing exam questions given to newly hired screeners,

the Inspector General concluded that the "some questions give away the answer and others are simply inane."

The General Accounting Office also raised troubling questions about TSA training and supervision. Although TSA has deployed basic screener training for new employees and remedial training to correct problems, it has not fully developed a program for recurrent training. It has also not fully developed a training program for supervisors. Perhaps most troubling of all, TSA knows very little about how its screeners are performing.

I understand that TSA is continuing to make improvements in these and other areas of security. I look forward to hearing from our witnesses today about TSA's progress and the challenges that it continues to face.

Statement of Congressman Elijah E. Cummings
Government Reform Hearing
On
"Knives, Box Cutters and Bleach: A Review of Passenger Screener Training, Testing and Supervision"
November 20, 2003 at 10:00 a.m.

Thank you, Mr. Chairman for holding this hearing.

In November of 2001, Congress created the Transportation Security Administration (TSA) within the Department of Transportation, in an effort to ensure safety for all modes of transportation, including aviation. This agency was created in the hopes that, through the development of a federal system for baggage screeners, air marshals, and other law enforcement personnel, U.S. citizens would be protected against another tragedy like the September 11th attacks.

Since then, billions of dollars have been spent on a wide range of initiatives designed to improve the security of commercial aviation. However, recent findings of the Government Accounting Office (GAO) and the Department of Homeland Security's (DHS) Office of Inspector General surrounding airport security, have found weaknesses in the testing, training, and performance of airport passenger and carry-on baggage screeners. In

addition, two of the private screening companies involved in the private pilot programs at two of the five pilot program airports, have expressed difficulty in achieving maximum performance due to rigid regulations imposed by TSA.

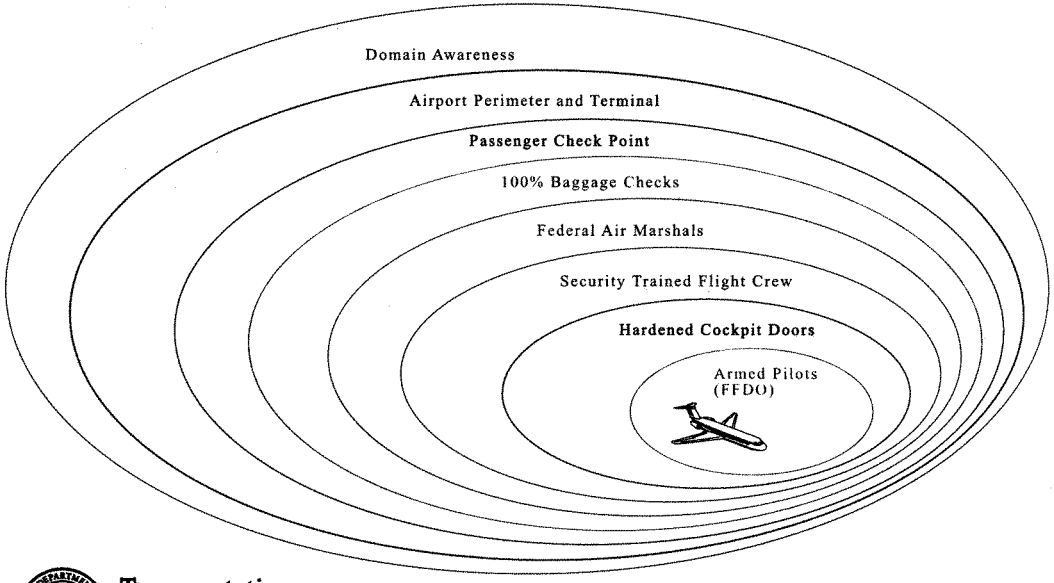
In an effort to ensure that travelers, especially as we approach the upcoming holiday season, are granted the highest level of safety possible, it is important that we address the reports by the GAO and the DHS. There is no doubt that the Transportation Security Agency has greatly improved civil aviation security – among other mandates, by requiring baggage screening with explosive detection systems, employing Federal Air Marshals on passenger flights, providing anti-hijack training for flight crews, and mandating cockpit doors and locks that cannot be opened by anyone other than flight crew. Yet, we cannot ignore the concerns posed by the GAO, DHS, and the private screening companies.

Today, every mode of transportation is a possible target for terrorism, and with that threat comes Congress' responsibility to continue to develop and enhance measures that increase the protection of both freight and passenger transportation. Public trust and confidence in our transportation system is

one of our nation's top priorities, so we must make sure that every effort to correct or prevent possible flaws in the current transportation security system is addressed. By measuring the success of the current TSA aviation security initiatives, reviewing the risk management plan TSA has established, and discussing the major changes needed to further improve aviation security, we can hopefully enjoy a more secure system.

With that said, I look forward to hearing from all of today's witnesses. Once again, thank you, Mr. Chairman, for holding this important hearing.

Aviation Rings of Security



Transportation
Security
Administration

Transportation Security Administration

Security Screeners

THEN and NOW

Issue	Screeners Then (Pre 9/11)	Screeners NOW (After TSA)
Employment	Contract employees	Federal employees
Selection Process	- Minimal Screening - No U.S. Citizenship requirement - Background Checks-minimal; no standards	- National comprehensive, competency based standards - Must be U.S. citizen or U.S. National - Extensive, standardized background investigation
Pay	Minimum wage; no benefits	Improved pay and benefits
Training	12 hours classroom, 40 hours On the Job	40 hours classroom, 60 hours On the Job, end of training certification required
Certification	None	Annual certification required
Supervision	Through air carriers	Direct Supervisory Control
Attrition	100-400% annually	13.6% (2003)

Transportation Security Administration

Aviation Security System of Systems

THEN and NOW

Security Program Component	THEN (Pre 9/11)	NOW (After TSA)
Airport Security Screeners	Contract screeners with no national program of operating procedures or standards	Federal screeners operating in consistent, standardized security protocols and who meet 100% of the national standards
FAMs	33 on International flights	Thousands on tens of thousands of monthly high-risk flights
Cockpit Doors	No hardened doors	All hardened doors
FFDOs	None	Hundreds now, more trained every week
Checked Baggage Screening	5% bags screened	100% of 1 billion bags screened annually
Federal Security Directors	None	158 FSDs for unified airport security
TIP	FAA 200 images	TSA 2,400 images
WTMD	Outdated technology	State of the art WTMD at all airports

TSA SCREENER IMPROVEMENTS

Transportation
Security
Administration

SHORT-TERM SCREENING IMPROVEMENT PLAN

CATEGORY	ACTION ITEM
PEOPLE	1. Increase FSD Support and Accountability 2. Enhance Training for Screeners and Supervisors 3. Increase Frequency of Internal Affairs Covert Testing 4. Continue to Pursue Human Performance Improvements
TECHNOLOGY	5. Continue to Identify New Screening Technology 6. Complete 100% Threat Image Projection System (TIP) Deployment 7. Continue IT Connectivity to Checkpoints and Training Computers
PROCESS	8. Refresh Aviation Operations Policy, Procedures and Practice 9. Improve Workforce Management Scheduling and Staffing

House Government Reform Committee

Oversight Hearing
"Knives, Box Cutters, and Bleach:
A Review of Passenger Screener Training, Testing and Supervision"

Thursday, November 20, 2003

Testimony of
The Coalition of American-Owned Security Companies (CASC)

Chairman Davis, Ranking Member Waxman and Members of the House Government Reform Committee, The Coalition of American-Owned Security Companies thanks you for this opportunity to provide testimony pursuant to the Committee's review of airport passenger screener training, testing and supervision.

The Coalition of American-Owned Security Companies is representative of the large, active and experienced American-owned private security industry in the United States. Coalition members include Barton Protective Services, Inc, Command Security Corporation, WSA Group, Inc. and GateSafe. Combined these American-owned private security companies have over a half-century of experience providing a vast array of security services for many governmental entities and industries, including a wide variety of airport services.

When the Aviation Transportation Security Act (ATSA) was passed in 2001, Congress mandated that the responsibility for passenger and baggage screening would move from airlines to the federal government. By November 19, 2002, Transportation Security Administration (TSA) screeners were in place at each of the 429 commercial-service airports in the United States.

Under ATSA, airports will be able to start applying to have screening services performed by private security companies under contract with TSA beginning in November 2004. ATSA also requires that such private security companies be owned and controlled by U.S. citizens to the extent that such companies exist. This provision presents the TSA, airports and private security companies with an exceptional opportunity to create a meaningful program that will incorporate the best practices and experiences of TSA, airports and the private security industry.

An Active and Vibrant U.S.-owned Private Screening Industry

There is an active and experienced American-owned airport security industry in the United States that is ready to meet today's security challenges. Private security companies have experience in every major airport in the country and have held contracts with every major airline. The industry has employed, recruited, and trained thousands of screening staff, and helped millions of passengers through security checkpoints throughout the United States.

As a part of the wider airport community, many American-owned private security companies also provide other airport services for airlines or airport clients. These range from security services—such as food and catering security, access control and perimeter patrol—to passenger services—such as skycaps, baggage handling, ticket verification and wheelchair assistance. Additionally, security companies provide security officers, access control and security consulting services to a multitude of industries beyond aviation.

In the new security environment that has emerged since the terrorist events of 2001, the private security industry has undergone significant change. The industry welcomed greater regulation and federal oversight following ATSA, and has embraced the movement toward the implementation of common professional standards for the security industry. Private security companies have the capacity, expertise and willingness to continue to serve in the airport security environment.

In 2002, TSA faced significant challenges in recruiting, training and mobilizing tens of thousands of screeners. Current budget and staff constraints continue to underscore the difficulty of running a uniform system across hundreds of different airports, each with its own unique challenges. Private sector capability can provide an additional resource for the government—for example, in staffing, customer service, security, operational efficiency and aviation industry experience.

Clearly, the private sector can play a valuable role in airport security, supported by strong federal oversight and regulation. This would provide an effective way forward for the aviation security industry as a whole.

The Opt-Out Program – A Unique Opportunity

ATSA provides airports with the opportunity to apply to opt-out of federal security provision beginning in November 2004. This presents the TSA, airports and private security companies with an exceptional opportunity to create a meaningful program that would incorporate the best practices and experiences of TSA, airports and the private security industry.

In defining the program, the input of airports and the private sector is essential. As an example, it would be beneficial for opt-out airports to be involved in the process of selecting screening companies. There should also be the opportunity for selected private

security companies to work under TSA regulation and enforcement as an integrated part of the airport community. This could help meet the desire, expressed by airport directors, for greater flexibility in determining work rules and procedures that more accurately reflect local needs.

Participation of private security companies in the evaluation of best practices for training, testing and supervision for airport passenger screeners in the opt-out airports should not be limited to the small universe of companies currently involved in TSA's five-airport private passenger screener pilot program. Evaluation of and input from many companies that make up the large number of American-owned private security companies can better identify best practices employed today.

With only one year before the opt-out process commences, TSA, airports and private security firms must move quickly to ensure that this program is implemented effectively and meets the needs of the public and the aviation community.

Why a Public-Private Sector Screening Partnership is the Way Forward

A public-private partnership incorporating TSA, security companies and airports brings mutual benefits and would facilitate effective resource management in the provision of safety and security to the public.

The benefits that screening companies can bring to this flagship public-private sector partnership are multifold:

Local Knowledge and Airport Community Experience

Private screening companies know and understand the airport environment. They are familiar with airport security stakeholders—the airport authorities, the airlines, local law enforcement, the federal security directors and other airport vendors—and recognize the need to work in partnership with other stakeholders. With experience in aviation, law enforcement, customer service, airport management and the military, this industry understands not only the importance of effective security but also the priorities of customer service, efficiency, and flexibility in airport operations.

Flexibility and Efficiency

Security staffing arrangements need to allow for variations in scheduling, such as the addition of new service, delays, cancellations, or peak season travel. The private sector has the capacity to increase or decrease staff quickly to cope with variable demand. In particular, because they frequently work in multiple areas of the airport, a private screening company may have the ability to pull cross-trained employees from appropriate areas during busy periods without impacting other operations.

Effective Training

Mobilization of large numbers of staff within a short time frame is common within the industry. This means that training needs can be carried out quickly and

effectively, to standards that meet TSA requirements. By conducting training on-site and including 'train the trainer' programs, private screening companies can speedily deploy staff in a way that may lead to cost-savings over the government's off-site training program. In addition, cross-training employees in multiple functions can ensure maximum flexibility during peak periods.

Conclusion

The U.S. private security industry is ready, willing and able to work with TSA and the airport community to make the opt-out program a success while continuing to ensure the safety and security of the American traveling public. The industry has both the experience and capacity to turn this public-private sector collaboration into a successful partnership that can be replicated across other industries.

The Coalition of American-Owned Security Companies welcomes the opportunity to work with TSA to forge a public-private partnership incorporating the best practices from TSA, security companies and airports for training, testing and supervision of airport passenger screeners. The Coalition looks forward to the creation of the airport opt-out program and offers the services of its member companies to TSA to ensure a program that is robust, efficient and above all else able to provide only the very best security to the American traveling public.

○