AVIATION SECURITY: ARE WE TRULY PROTECTED? PART I AND A FRONTLINE PERSPECTIVE ON THE NEED FOR ENHANCED HUMAN RESOURCES AND EQUIPMENT, PART II

HEARING

BEFORE THE

SUBCOMMITTEE ON TRANSPORTATION SECURITY AND INFRASTRUCTURE PROTECTION

OF THE

COMMITTEE ON HOMELAND SECURITY HOUSE OF REPRESENTATIVES

ONE HUNDRED TENTH CONGRESS

FIRST SESSION

OCTOBER 16, 2007 AND NOVEMBER 1, 2007

Serial No. 110–77

Printed for the use of the Committee on Homeland Security

Available via the World Wide Web: http://www.gpoaccess.gov/congress/index.html

U.S. GOVERNMENT PRINTING OFFICE
48–972 PDF WASHINGTON : 2009

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) 512–2104 Mail: Stop IDCC, Washington, DC 20402–0001

COMMITTEE ON HOMELAND SECURITY

BENNIE G. THOMPSON, Mississippi, *Chairman*

LORETTA SANCHEZ, California,
EDWARD J. MARKEY, Massachusetts
NORMAN D. DICKS, Washington
JANE HARMAN, California
PETER A. DEFAZIO, Oregon
NITA M. LOWEY, New York
ELEANOR HOLMES NORTON, District of Columbia
ZOE LOFGREN, California
SHEILA JACKSON LEE, Texas
DONNA M. CHRISTENSEN, U.S. Virgin Islands
BOB ETHERIDGE, North Carolina
JAMES R. LANGEVIN, Rhode Island
HENRY CUELLAR, Texas
CHRISTOPHER P. CARNEY, Pennsylvania
YVETTE D. CLARKE, New York
AL GREEN, Texas
ED PERLMUTTER, Colorado
VACANCY

PETER T. KING, New York
LAMAR SMITH, Texas
CHRISTOPHER SHAYS, Connecticut
MARK E. SOUDER, Indiana
TOM DAVIS, Virginia
DANIEL E. LUNGREN, California
MIKE ROGERS, Alabama
BOBBY JINDAL, Louisiana
DAVID G. REICHERT, Washington
MICHAEL T. MCCAUL, Texas
CHARLES W. DENT, Pennsylvania
GINNY BROWN-WAITE, Florida
MARSHA BLACKBURN, Tennessee
GUS M. BILIRAKIS, Florida
DAVID DAVIS, Tennessee

JESSICA HERRERA-FLANIGAN, *Staff Director & General Counsel*
ROSALINE COHEN, *Chief Counsel*
MICHAEL TWINCHEK, *Chief Clerk*
ROBERT O'CONNOR, *Minority Staff Director*

SUBCOMMITTEE ON TRANSPORTATION SECURITY AND INFRASTRUCTURE PROTECTION

SHEILA JACKSON LEE, Texas, *Chairwoman*

EDWARD J. MARKEY, Massachusetts
PETER A. DEFAZIO, Oregon
ELEANOR HOLMES NORTON, District of Columbia
YVETTE D. CLARKE, New York
ED PERLMUTTER, Colorado
BENNIE G. THOMPSON, Mississippi *(Ex Officio)*

DANIEL E. LUNGREN, California
GINNY BROWN-WAITE, Florida
MARSHA BLACKBURN, Tennessee
GUS M. BILIRAKIS, Florida
PETER T. KING, New York *(Ex Officio)*

MATHEW WASHINGTON, *Director*
ERIN DASTE, *Counsel*
NATALIE NIXON, *Deputy Chief Clerk*
COLEY O'BRIEN, *Senior Counsel*

CONTENTS

AVIATION SECURITY: ARE WE TRULY PROTECTED?
PART I

Tuesday, October 16, 2007

U.S. HOUSE OF REPRESENTATIVES,
COMMITTEE ON HOMELAND SECURITY,
SUBCOMMITTEE ON TRANSPORTATION SECURITY AND
INFRASTRUCTURE PROTECTION,
Washington, DC.

The subcommittee met, pursuant to call, at 2:23 p.m., in Room 311, Cannon House Office Building, Hon. Sheila Jackson Lee [chairwoman of the subcommittee] presiding.

Present: Representatives Jackson Lee, Markey, DeFazio, Clarke, Perlmutter, and Lungren.

Also present: Representative Pascrell.

Ms. JACKSON LEE. [Presiding.] The subcommittee will come to order.

The subcommittee is meeting today to receive testimony on the Transportation Security Administration coordination with the Federal Aviation Administration when incidents move from a safety incident to a security incident and general aviation security. We also have the Government Accountability Office, GAO, before us today as well.

However, before I begin, I ask for unanimous consent that Mr. Pascrell, a member of the full committee, to sit and question the panels during today's hearings. Without objection: so ordered.

Welcome, Mr. Pascrell. You have never left us and we are delighted to have you here with us today.

Let me acknowledge the presence as well of Mr. Perlmutter, a member of the subcommittee, and Mr. DeFazio, a member of the subcommittee, and of course, the ranking member.

As we all know, the Congress, and specifically this committee, continue to have serious concerns regarding aviation security in the United States since September 11. The ensuing debates in Congress continue to focus on the degree of federal involvement needed to improve aviation security and maintain public confidence in air travel. This ongoing debate started with the Aviation Transportation Security Act, which established the Transportation Security Administration in response to the September 11, 2001 attacks on the World Trade Center and the Pentagon. I might add, long overdue.

At the beginning, TSA was headed by an under secretary of transportation for security within the Department of Transpor-

tation. Within 3 months after enactment of the ATSA, the responsibilities for aviation security were transferred from the Federal Aviation Administration to the TSA. It was no longer FAA, but TSA was charged with managing a federal screening workforce and requiring screening of checks bags using explosive detection systems.

Now, let me say that I am very proud and pleased at the work of our chairman, Chairman Thompson and Chairman Oberstar, for we have coordinated and collaborated. I have good working relationships with the chair of the Subcommittee on Aviation, Mr. Costello, and we have indicated that we look forward to working together. But it is a responsibility of the TSA to address the question of aviation security. However, it is a collaborative effort and it must be done with the two principal witnesses that are here that will offer their thoughts and testimony as to the effectiveness of that collaboration, of course, with the insight of the GAO.

ATSA also significantly expanded the Federal Air Marshal Program requiring that all cockpit doors be strengthened and provided for various other aviation security measures. Let me also indicate that in our next hearing, we will address the question of the issues of the Federal Air Marshal Program, training, other personnel matters, effectiveness, the marshals' insight into whether or not the program is as strong as it should be, and how we can strengthen their service so that they can strengthen aviation security.

We will also look at flight attendants and the training that is necessary that still has not been accomplished these many years later.

This was not the final step in the transformation of the TSA. Later, the Homeland Security Act of 2002 established the Department of Homeland Security and completely removed the TSA from DOT in placing it in DHS. While there has always been a distinction between TSA and the FAA, these two entities will always have a connection. The aviation community relies on FAA for safety and TSA for security. However, today I want to explore, as I previously said, how these two distinctive agencies coordinate when an accident or incident goes from being a safety concern to a security concern.

The committee wants to make sure that the FAA and the TSA are aligned and work very closely together in terms of understanding and implementing their respective roles in responding to aviation security threats. In addition to the coordination between the FAA and the TSA, I am very interested in how air traffic controllers are trained to deal with security incidents and what steps we can take to make sure that air traffic controllers have the training to be able to deal with the security threat.

As you know, training of frontline workers is of paramount importance to this committee. In all modes of transportation, we must ensure that workers have the knowledge and skill to respond to a multitude of security issues. We need assurances from the TSA that aviation TSOs are indeed getting this training.

But it is not just coordination I am worried about. Many believe that the risk-based approach implemented by the TSA places an overemphasis on allocating resources to screening airline passengers and have left the system vulnerable to attacks in other

areas, namely air cargo operations, airport access controls, and protecting airliners from shoulder-fired missiles.

In essence, these critics argue that the implementation of aviation security policy since September 11, 2001 has focused too heavily on protecting aircraft from past attack scenarios such as suicide hijackings and luggage bombs carried out by airline passengers, and has not given enough attention to other potential vulnerabilities, which speaks to the question of air traffic controllers and certainly speaks to the question of whether we are fully staffed and trained, and what are the vulnerabilities of the numbers of air traffic controllers that we have today.

Supporting our suspicions that TSA is missing the mark, the GAO identified seven performance expectations which have not been achieved, specifically airport perimeter security, control access to airport secured areas—the Phoenix incident, biometric identifier systems, international passenger pre-screening process, and technologies to screen air cargo.

As members of Congress, and more specifically as members of the Committee on Homeland Security, we have a responsibility to make sure our planes and airports and other modes of transportation are safe. I would venture to say that if, as we have all speculated the possibility, a horrific incident occurs, I would imagine Americans would ask the question, "What did the Committee on Homeland Security and what did the Department of Homeland Security do to prevent this horrific incident?"

We are at a crossroads where we must take action to find out what is the best way to provide a safe, secure and functional aviation system. If we do not put effective security measures in place, our nation may very well be the victim of another attack, which in turn will cause a major economic disruption and an avoidance of commercial aviation. We saw what happened after 9/11. We must continually earn the confidence of the flying public in order to ensure that the public continues to enjoy the freedom of mobility that flying provides. We must demonstrate to them that our nation's airports are secure.

Let me finally say that we understand there have been significant incidences of slowdowns and a number of problems that have occurred to the traveling aviation public as it relates to the services, as has been pointed out by airlines, of air traffic controllers. Many argue that that is a safety question or a question of logistics. I argue that it is as much a security concern as it is a safety concern, not because of the witnesses who are here today, but I believe the system is broken and we have an obligation to fix it in order to secure the American public.

With this, I am delighted to yield to the ranking member of the subcommittee to deliver his remarks, Mr. Lungren of California.

Mr. LUNGREN. Thank you very much, Madam Chairwoman. Maybe I can be king for a day.

[Laughter.]

I want to thank you for scheduling today's hearing on this important issue, aviation security. When you started talking about the public's view of things, I am reminded of a recent poll that I saw in which 73 percent of the American people believe that the U.S.

government has been effective in preventing a terrorist attack in America since 9/11.

At the same time, the same poll shows that 56 percent of the American people believe that they are less safe today, that is, that we are becoming less safe, rather than safer. How do you put those two things together? I think it is because they recognize that we have taken steps that have been effective, that we are indeed in many ways safer, but that the threat remains and the threat is every bit as intense.

That is why I think it is incumbent on those of us in the Congress to have the urgency that seems to be indicated by the American people's attitude both towards the effective job that we have done in the past, but the continuing threat that remains. The airplane has been and continues to be the terrorists' weapon of choice when carrying out attacks on our country. The 2006 liquid explosives plot uncovered in London reminded us that commercial aircraft remains a favorite weapon of the terrorists.

We in Congress are often quick to criticize our government agencies and their employees. Today, however, I am pleased to congratulate TSA and its many dedicated employees on achieving 17 out of the 24 GAO aviation security performance expectations in their most recent report. Maybe it is just I like to see the glass half full rather than half empty.

It shows progress, in my estimation, although much more remains to be done. Congress has provided substantial funding for aviation security. While much remains to be done, it is reassuring to see the progress TSA has made in securing our airlines. One of Congress's first mandates after 9/11 was for TSA to screen 100 percent of airline passengers and their baggage. This goal has been achieved. While Americans still don't like the inconvenience, they I think understand intuitively that it is necessary to do that in order for us to have safer skies.

Now, TSA is strengthening its focus on passenger pre-screening, Secure Flight. It plans to take control of passenger information matching from the airlines against the terror watch list prior to the aircraft's departure. That is improvement. This involves effective use of intelligence sources to identify possible terrorist threats, and I fully support these efforts.

I might just say parenthetically, the whole idea of intelligence is why the vote that we are going to have this week on Pfizer is so important. If you look at a risk-based assessment, it is threat vulnerability and consequence. Vulnerability and consequence are things within our domain of information. Threat is only within our domain of information based on the amount of intelligence we have, how effectively we identify it, and how we put it together, i.e. connecting the dots. That is why this vote this week is so important.

Registered traveler—another TSA change that would immeasurably improve the travel experience for airline customers, and at the same time provide security, in my judgment, is a fully implemented registered traveler program. Congress directed TSA in 2002 to establish a registered traveler program, allowing passengers who provide their biometric and biographic information, access to expedited security processing at the checkpoint.

Now, 5 years later, the promise of expedited processing for registered travelers is at best a mirage. I find it difficult when my wife says to me at home, "What is the matter with you guys? It seems to me that is a relatively simple thing to do. We would like to get it done. Why can't you get it done?" I am still trying to get the answer so that I may go home and answer my wife. I want to tell you, that is a high priority in my life.

Instead of facilitating travel for participants, TSA is making it more difficult, in my judgment, by requiring double identification for the registered traveler, while demanding only a single government photo ID from the guy off the street. I have heard the arguments that have been made. I don't understand them.

I am a strong believer that intelligence is our best weapon against terrorism, as I previously said. The more personal passenger information we have, the better our chances for identifying travelers who may pose a threat. Shouldn't we be encouraging programs that provide us with greater intelligence, particularly when that information is given voluntarily?

I am also disturbed by the trend of some in this Congress away from the risk-based security model that we have followed in this committee since 9/11. New screening proposals advocated by some for passenger air cargo, maritime cargo containers, and airport employees seem to think that the magic of 100 percent by some definitions is just that, magic. I am concerned about whether or not we are looking for the silver bullet that we can never find.

I am convinced that we need to send valuable TSA funding and personnel resources in a layered approach, the most effective approach, the smart approach. We will not be able to defeat those who want to destroy us by out-manning them. We will by the intelligent use of our technology, our information, and our analysis.

We need to ensure that as we do this, we do not allow them either to destroy us or to destroy our commerce in the process. We can do this, I am absolutely convinced. Multi-layered, risk-based security guided by intelligence is still the best defense against the evolving threat of terrorism.

I thank the chairwoman.

Ms. JACKSON LEE. I thank the distinguished gentleman for his comments.

Let me also acknowledge the presence of the distinguished gentlelady from New York, Congresswoman Yvette Clarke.

At this time, I would like to welcome our panel of witnesses. Our first witness will be Ms. Cathy Berrick, Director of Homeland Security and Justice Issues for the General Accountability Office. In this capacity, she oversees the GAO's reviews of aviation and surface transportation security matters, and has developed broad knowledge of transportation security practices and related federal policies, and federal and private sector roles and responsibilities.

She has leveraged this expertise to lead numerous reviews of the department and TSA initiatives to strengthen the security of U.S. transportation systems and to interpret the complex array of legislation passed and policies instituted in the aftermath of the September 11, 2001 terrorist attacks. Ms. Berrick, welcome.

Our second witness is Assistant Secretary for Transportation Security Kip Hawley. Assistant Secretary Hawley, as usual, it is al-

ways a pleasure to have you, and we always look forward to your forthright testimony. We thank you very much for your presence here today. Let me just suggest to you that your very presence and your very position allows us simply to introduce you as the Assistant Secretary of Transportation Security, so the shortness of your introduction does not in any way measure your importance.

The final witness of this panel is Mr. Franklin Hatfield, Director of the Operations Security Office for the FAA. Mr. Hatfield is responsible for integrating all aviation and aerospace security into the national airspace system. He serves as the nexus between operational intelligence and the NSA, and is responsible for balancing the needs of national security with the operational and economic demands of aviation commerce.

Let me say, Mr. Hatfield, that we are delighted that you are here. Let me make a personal statement that we will look forward to the administrator's presence at some future time before this committee. The absence of the administrator is certainly not one that is going to be accepted on a long-term basis, but we thank you for the responsibilities that you have and your presence here today.

I am now asking that the witnesses, without objection, will have their full statements inserted into the record. I now ask each witness to summarize his or her statement for 5 minutes, beginning with Director Berrick from the Government Accountability Office.

Thank you very much again.

STATEMENT OF CATHLEEN A. BERRICK, DIRECTOR, HOMELAND SECURITY AND JUSTICE ISSUES, U.S. GOVERNMENT ACCOUNTABILITY OFFICE

Ms. BERRICK. Thank you, Madam Chair, Representative Lungren and members of the subcommittee, for inviting me here to discuss GAO's work assessing TSA's progress in securing commercial aviation.

In August, 2007, shortly after the Department of Homeland Security's 4-year anniversary, we reported to this committee on DHS's progress in satisfying its key mission and management functions, including TSA's efforts in securing aviation and surface modes of transportation.

We based our assessment on over 400 reports and testimonies we have completed assessing DHS's operations, and by determining whether DHS generally achieved or generally did not achieve key performance expectations set out for them by Congress, the administration, and the department itself. Overall, we reported that TSA has made moderate progress in securing commercial aviation. More specifically, we found that TSA generally achieved about 70 percent of the 24 performance expectations established for them.

In terms of progress, TSA is taking considerable action in hiring, deploying, training and measuring the performance of its aviation security workforce. These efforts include the development of robust training programs for TSOs or screeners, including enhanced explosives detection training and standards for determining appropriate TSO staffing levels at airports.

TSA has also made significant progress in balancing security and efficiency in developing checkpoint screening procedures, deploying checked baggage screening equipment, and enhancing covert test-

ing to assess vulnerabilities in the screening of passengers and checked baggage.

TSA is also researching and developing more effective and efficient screening technologies, and has taken action to strengthen the security of domestic air cargo through the development of security requirements and other initiatives.

However, we find that DHS and TSA has made less progress in securing airport perimeters and access to restricted areas, deploying technologies to detect explosives at checkpoints and to screen air cargo, and building a system to pre-screen airline passengers against terrorist watch lists for domestic flights, although progress is being made in all of these areas.

One of the most critical areas in which limited progress has been made is in the deployment of technologies at airport checkpoints to detect explosives on passengers and in their carry-on bags. Although DHS is developing and testing technologies, the department has reported that the extensive deployment of new checkpoint technologies will not be realized for another 2 years.

In addition, although TSA has taken action to strengthen the security of airport perimeters and access controls, covert tests continue to identify weaknesses in this area, and DHS did not identify to us how its actions have addressed all relevant legislative requirements, as well as respond to our prior recommendations.

A variety of cross-cutting issues have affected DHS's and TSA's efforts in implementing its mission and management functions. These include developing results-oriented goals and measures to assess performance, developing and integrating a risk-based approach to guide investment decisions, and establishing effective frameworks and mechanisms for sharing information and coordinating with stakeholders. It will be important for the department to continue to address these issues as it moves forward.

In closing, TSA has made considerable progress in securing commercial aviation and its efforts should be commended. However, the agency still has more work to do in some key areas, most especially related to the deployment of technologies to screen for explosives at checkpoints and in air cargo, and with respect to the security of surface transportation modes, more fully defining its regulatory role.

We are currently reviewing many of these key areas for this committee and will continue to report to the Congress and the public on the results of our work.

Madam Chair, this concludes my opening statement. Thank you.

[The statement of Ms. Berrick follows:]

United States Government Accountability Office

GAO

Testimony Before the Subcommittee on Transportation Security and Infrastructure Protection, House Committee on Homeland Security

For Release on Delivery
Expected at 2:00 p.m. EDT
Tuesday, October 16, 2007

AVIATION SECURITY

DHS Has Made Progress in Securing the Commercial Aviation System, but Key Challenges Remain

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

GAO-08-139T

Madam Chair and Members of the Subcommittee:

I appreciate the opportunity to participate in today's hearing to discuss the Department of Homeland Security's (DHS) progress and challenges in securing our nation's aviation system. The Transportation Security Administration (TSA), originally established as an agency within the Department of Transportation in 2001 but now a component within DHS, is charged with securing the transportation network while also ensuring the free movement of people and commerce. TSA has primary responsibility for security in all modes of transportation and since its inception has developed and implemented a variety of programs and procedures to secure the commercial aviation system. Other DHS components, federal agencies, state and local governments, and the private sector also play a role in aviation security. For example, the U.S. Customs and Border Protection (CBP) has responsibility for conducting passenger prescreening—in general, the matching of passenger information against terrorist watch lists prior to an aircraft's departure—for international flights operating to or from the United States, as well as inspecting inbound air cargo upon its arrival in the United States. In accordance with TSA requirements, airport authorities are responsible for implementing measures to secure access to restricted airport areas as well as airport perimeters, while air carriers are responsible for inspecting air cargo, among other things.

My testimony today will focus on: (1) the progress TSA and other DHS components have made in securing the nation's commercial aviation system and (2) challenges that have impeded DHS's (and, as they relate to transportation security, TSA) efforts to implement its mission and management functions. My comments are based on issued GAO reports and testimonies addressing the security of the nation's aviation system, including an August 2007 report that highlights the progress DHS has made in implementing its mission and management functions.[1] In this report, we reviewed the extent to which DHS has taken actions to achieve

[1] GAO, *Department of Homeland Security: Progress Report on Implementation of Mission and Management Functions*, GAO-07-454 (Washington, D.C.: August 2007); GAO, *Department of Homeland Security: Progress Report on Implementation of Mission and Management Functions*, GAO-07-1081T (Washington, D.C.: September 2007); and GAO, *Department of Homeland Security: Progress Report on Implementation of Mission and Management Functions*, GAO-07-1240T (Washington, D.C.: September 2007).

Madam Chair and Members of the Subcommittee:

I appreciate the opportunity to participate in today's hearing to discuss the Department of Homeland Security's (DHS) progress and challenges in securing our nation's aviation system. The Transportation Security Administration (TSA), originally established as an agency within the Department of Transportation in 2001 but now a component within DHS, is charged with securing the transportation network while also ensuring the free movement of people and commerce. TSA has primary responsibility for security in all modes of transportation and since its inception has developed and implemented a variety of programs and procedures to secure the commercial aviation system. Other DHS components, federal agencies, state and local governments, and the private sector also play a role in aviation security. For example, the U.S. Customs and Border Protection (CBP) has responsibility for conducting passenger prescreening—in general, the matching of passenger information against terrorist watch lists prior to an aircraft's departure—for international flights operating to or from the United States, as well as inspecting inbound air cargo upon its arrival in the United States. In accordance with TSA requirements, airport authorities are responsible for implementing measures to secure access to restricted airport areas as well as airport perimeters, while air carriers are responsible for inspecting air cargo, among other things.

My testimony today will focus on: (1) the progress TSA and other DHS components have made in securing the nation's commercial aviation system and (2) challenges that have impeded DHS's (and, as they relate to transportation security, TSA) efforts to implement its mission and management functions. My comments are based on issued GAO reports and testimonies addressing the security of the nation's aviation system, including an August 2007 report that highlights the progress DHS has made in implementing its mission and management functions.[1] In this report, we reviewed the extent to which DHS has taken actions to achieve

[1] GAO, *Department of Homeland Security: Progress Report on Implementation of Mission and Management Functions*, GAO-07-454 (Washington, D.C.: August 2007); GAO, *Department of Homeland Security: Progress Report on Implementation of Mission and Management Functions*, GAO-07-1081T (Washington, D.C.: September 2007); and GAO, *Department of Homeland Security: Progress Report on Implementation of Mission and Management Functions*, GAO-07-1240T (Washington, D.C.: September 2007).

performance expectations in each of its mission and management areas that we identified from legislation, Homeland Security Presidential Directives, and DHS strategic planning documents. Based primarily on our past work, we made a determination regarding whether DHS generally achieved or generally did not achieve the key elements of each performance expectation. An assessment of "generally achieved" indicates that DHS has taken sufficient actions to satisfy most elements of the expectation; however, an assessment of "generally achieved" does not signify that no further action is required of DHS or that functions covered by the expectation cannot be further improved or enhanced. Conversely, an assessment of "generally not achieved" indicates that DHS has not yet taken actions to satisfy most elements of the performance expectation. In determining the department's overall level of progress in achieving performance expectations in each of its mission and management areas, we concluded whether the department had made limited, modest, moderate, or substantial progress.[2] These assessments of progress do not reflect, nor are they intended to reflect, the extent to which actions by DHS and its components have made the nation more secure. We conducted our work in accordance with generally accepted government auditing standards.

Summary

Within DHS, TSA is the agency with primary responsibility for securing the transportation sector and has undertaken a number of initiatives to strengthen the security of the nation's commercial aviation system. In large part, these efforts have been driven by legislative mandates designed to strengthen the security of commercial aviation following the September 11, 2001, terrorist attacks. In August 2007, we reported that DHS had made moderate progress in securing the aviation transportation network, but that more work remains.[3] Specifically, of the 24 performance expectations we identified for DHS in the area of aviation security, we reported that it has generally achieved 17 of these expectations and has generally not achieved 7 expectations.

[2] Limited progress: DHS has taken actions to generally achieve 25 percent or less of the identified performance expectations. Modest progress: DHS has taken actions to generally achieve more than 25 percent but 50 percent or less of the identified performance expectations. Moderate progress: DHS has taken actions to generally achieve more than 50 percent but 75 percent or less of the identified performance expectations. Substantial progress: DHS has taken actions to generally achieve more than 75 percent of the identified performance expectations.

[3] GAO-07-454.

DHS, primarily through TSA, has made progress in many areas related to securing commercial aviation, and their efforts should be commended. Meeting statutory mandates to screen airline passengers and 100 percent of checked baggage alone was a tremendous challenge. To do this, TSA initially hired and deployed a federal workforce of over 50,000 passenger and checked baggage screeners, and installed equipment at the nation's more than 400 commercial airports to provide the capability to screen all checked baggage using explosive detection systems, as mandated by law. TSA has since turned its attention to, among other things, strengthening passenger prescreening—in general, the matching of passenger information against terrorist watch lists prior to an aircraft's departure; more efficiently allocating, deploying, and managing the transportation security officer (TSO)—formerly known as screener—workforce; strengthening screening procedures; developing and deploying more effective and efficient screening technologies; and improving domestic air cargo security. In addition to TSA, CBP has also taken steps to strengthen passenger prescreening for passengers on international flights operating to or from the United States, as well as inspecting inbound air cargo upon its arrival in the United States. DHS's Science and Technology (S&T) Directorate has also taken actions to research and develop aviation security technologies.

While these efforts have helped to strengthen the security of the commercial aviation system, DHS still faces a number of key challenges that need to be addressed to meet expectations set out for them by the Congress, the Administration, and the Department itself. For example, TSA has faced challenges in developing and implementing its passenger prescreening system, known as Secure Flight, and has not yet completed development efforts. As planned, this program would initially assume from air carriers the responsibility for matching information on airline passengers traveling domestically against terrorists watch lists. In addition, while TSA has taken actions to enhance perimeter security at airports, these actions may not be sufficient to provide for effective security. TSA has also begun efforts to evaluate the effectiveness of security-related technologies, such as biometric identification systems. However, TSA has not developed a plan for implementing new technologies to meet the security needs of individual airports and the commercial airport system as a whole. Further, TSA has not yet deployed checkpoint technologies to address key existing vulnerabilities, and has not yet developed and implemented technologies needed to screen air cargo.

A variety of cross-cutting issues have affected DHS's and, as they relate to transportation security, TSA's efforts in implementing its mission and management functions. These key issues include agency transformation, strategic planning and results management, risk management, information sharing, and stakeholder coordination. In working towards transforming the department into an effective and efficient organization, DHS and its components have not always been transparent, which has affected our ability to perform our oversight responsibilities in a timely manner. They have also not always implemented effective strategic planning efforts, fully developed performance measures, or put into place structures to help ensure that they are managing for results. In addition, DHS and its components can more fully adopt and apply a risk management approach in implementing its security mission and core management functions.[4] They could also better share information with federal, state, and local governments and private sector entities, and more fully coordinate its activities with key stakeholders.

Background

The Aviation and Transportation Security Act (ATSA), enacted in November 2001, created TSA and gave it responsibility for securing all modes of transportation.[5] TSA's aviation security mission includes strengthening the security of airport perimeters and restricted airport areas; hiring and training a screening workforce; prescreening passengers against terrorist watch lists; and screening passengers, baggage, and cargo at the over 400 commercial airports nation-wide, among other responsibilities. While TSA has operational responsibility for physically screening passengers and their baggage, TSA exercises regulatory, or oversight, responsibility for the security of airports and air cargo. Specifically, airports, air carriers, and other entities are required to implement security measures in accordance with TSA-issued security requirements, against which TSA evaluates their compliance efforts.

TSA also oversees air carriers' efforts to prescreen passengers—in general, the matching of passenger information against terrorist watch lists— prior

[4] A risk management approach entails a continuous process of managing risk through a series of actions, including setting strategic goals and objectives, assessing risk, evaluating alternatives, selecting initiatives to undertake, and implementing and monitoring those initiatives.

[5] Pub. L. No. 107-71, 115 Stat. 597 (2001).

to an aircraft's departure. TSA plans to take over operational responsibility for this function with the implementation of its Secure Flight program initially for passengers traveling domestically. CBP has responsibility for conducting passenger prescreening for airline passengers on international flights departing from and bound for the United States,[6] while DHS's Science and Technology Directorate is responsible for researching and developing technologies to secure the transportation sector.

DHS Has Made Progress in Securing the Nation's Commercial Aviation System, but More Work Remains

DHS, primarily through the efforts of TSA, has undertaken numerous initiatives since its inception to strengthen the security of the nation's commercial aviation system. In large part, these efforts have been affected by legislative mandates designed to strengthen the security of commercial aviation following the September 11, 2001 terrorist attacks. These efforts have also been affected by events external to the department, including the alleged August 2006 terrorist plot to blow up commercial aircraft bound from London to the United States. For example, TSA has undertaken efforts to hire, train, and deploy a screening workforce; and screen passengers, baggage, and cargo. Although TSA has taken important actions to strengthen aviation security, the agency has faced difficulties in implementing an advanced, government-run passenger prescreening program for domestic flights, and in developing and implementing technology to screen passengers at security checkpoints and cargo placed on aircraft, among other areas. As shown in table 1, we identified 24 performance expectations for DHS in the area of aviation security, and found that overall, DHS has made moderate progress in meeting these expectations. Specifically, we found that DHS has generally achieved 17 performance expectations and has generally not achieved 7 performance expectations. We identified these performance expectations through reviews of key legislation, Homeland Security Presidential Directives, and DHS strategic planning documents.

[6] Currently, air carriers departing the United States are required to transmit passenger manifest information to CBP no later than 15 minutes prior to departure but, for flights bound for the United States, air carriers are not required to transmit the information until 15 minutes after the flight's departure (in general, after the aircraft is in flight). See 19 C.F.R. §§ 122.49a, 122.75a. In a final rule published in the *Federal Register* on August 23, 2007, CBP established a requirement for all air carriers to either transmit the passenger manifest information to CBP no later than 30 minutes prior to the securing of the aircraft doors (that is, prior to the flight being airborne), or transmit manifest information on an individual basis as each passenger checks in for the flight up to but no later than the securing of the aircraft. See 72 Fed. Reg. 48,320 (Aug. 23, 2007). This requirement is to take effect on February 19, 2008.

Table 1: Performance Expectations and Progress Made in Aviation Security

Performance expectation	Assessment		
	Generally achieved	Generally not achieved	No assessment made
Aviation security strategic approach			
Implement a strategic approach for aviation security functions	✓		
Airport perimeter security and access controls			
Establish standards and procedures for effective airport perimeter security		✓	
Establish standards and procedures to effectively control access to airport secured areas		✓	
Establish procedures for implementing biometric identifier systems for airport secured areas access control		✓	
Ensure the screening of airport employees against terrorist watch lists	✓		
Aviation security workforce			
Hire and deploy a federal screening workforce	✓		
Develop standards for determining aviation security staffing at airports	✓		
Establish standards for training and testing the performance of airport screener staff	✓		
Establish a program and requirements to allow eligible airports to use a private screening workforce	✓		
Train and deploy federal air marshals on high-risk flights	✓		
Establish standards for training flight and cabin crews	✓		
Establish a program to allow authorized flight deck officers to use firearms to defend against any terrorist or criminal acts	✓		
Passenger prescreening			
Establish policies and procedures to ensure that individuals known to pose, or suspected of posing, a risk or threat to security are identified and subjected to appropriate action	✓		
Develop and implement an advanced prescreening system to allow DHS to compare domestic passenger information to the Selectee List and No Fly List		✓	
Develop and implement an international passenger prescreening process to compare passenger information to terrorist watch lists before aircraft departure		✓	
Checkpoint screening			
Develop and implement processes and procedures for physically screening passengers at airport checkpoints	✓		
Develop and test checkpoint technologies to address vulnerabilities	✓		
Deploy checkpoint technologies to address vulnerabilities		✓	

Performance expectation	Assessment		
	Generally achieved	Generally not achieved	No assessment made
Checked Baggage screening			
Deploy explosive detection systems (EDS) and explosive trace detection (ETD) systems to screen checked baggage for explosives	✓		
Develop a plan to deploy in-line baggage screening equipment at airports	✓		
Pursue the deployment and use of in-line baggage screening equipment at airports	✓		
Air cargo security			
Develop a plan for air cargo security	✓		
Develop and implement procedures to screen air cargo	✓		
Develop and implement technologies to screen air cargo		✓	
Total	**17**	**7**	**0**

Source: GAO analysis.

Aviation Security Strategic Approach. We concluded that DHS has generally achieved this performance expectation. In our past work, we reported that TSA identified and implemented a wide range of initiatives to strengthen the security of key components of the commercial aviation system. These components are interconnected and each is critical to the overall security of commercial aviation.[7] More recently, in March 2007, TSA released its National Strategy on Aviation Security and six supporting plans that provided more detailed strategic planning guidance in the areas of systems security; operational threat response; systems recovery; domain surveillance; and intelligence integration and domestic and international outreach. According to TSA officials, an Interagency Implementation Working Group was established under TSA leadership in January 2007 to initiate implementation efforts for the 112 actions outlined in the supporting plans.

Airport Perimeter Security and Access Controls. We concluded that DHS has generally achieved one, and has generally not achieved three, of the performance expectations in this area. For example, TSA has taken

[7] For more information, see GAO, *Aviation Security: Enhancements Made in Passenger and Checked Baggage Screening, but Challenges Remain*, GAO-06-371T (Washington, D.C: April 2006).

action to ensure the screening of airport employees against terrorist watch lists by requiring airport operators to compare applicants' names against the No Fly and Selectee Lists.[8] However, in June 2004, we reported that although TSA had begun evaluating commercial airport perimeter and access control security through regulatory compliance inspections, covert testing of selected access procedures, and vulnerability assessments at selected airports, TSA had not determined how the results of these evaluations could be used to make improvements to the nation's airport system as a whole. We further reported that although TSA had begun evaluating the controls that limit access into secured airport areas, it had not completed actions to ensure that all airport workers in these areas were vetted prior to being hired and trained.[9] More recently, in March 2007, the DHS Office of Inspector General, based on the results of its access control testing at 14 domestic airports across the nation, made various recommendations to enhance the overall effectiveness of controls that limit access to airport secured areas.[10] In March through July 2007, DHS provided us with updated information on procedures, plans, and other efforts it had implemented to secure airport perimeters and strengthen access controls, including a description of its Aviation Direct Access Screening Program. This program provides for TSOs to randomly screen airport and airline employees and employees' property and vehicles as they enter the secured areas of airports for the presence of explosives, incendiaries, weapons, and other items of interest as well as improper airport identification. However, DHS did not provide us with evidence that these actions provide for effective airport perimeter security, nor information on how the actions addressed all relevant requirements established by law and in our prior recommendations.

Regarding procedures for implementing biometric identification systems, we reported that TSA had not developed a plan for implementing new

[8] For more information, see GAO, Aviation Security: Transportation Security Administration Has Made Progress in Managing a Federal Security Workforce and Ensuring Security at U.S. Airports, but Challenges Remain, GAO-06-597T , (Washington, D.C.: April 2006) and GAO, Aviation Security: Further Steps Needed to Strengthen the Security of Commercial Airport Perimeters and Access Controls, GAO-04-728 (Washington, D.C.: June 2004).

[9] GAO-06-597T and GAO-04-728.

[10] Department of Homeland Security Office of Inspector General, Audit of Access to Airport Secured Areas (Unclassified Summary), OIG-07-35 (Washington, D.C.: March 2007).

technologies to meet the security needs of individual airports and the commercial airport system as a whole.[11]

In December 2004 and September 2006, we reported on the status of the development and testing of the Transportation Worker Identification Credential program (TWIC)[12] – DHS's effort to develop biometric access control systems to verify the identity of individuals accessing secure transportation areas. Our 2004 report identified challenges that TSA faced in developing regulations and a comprehensive plan for managing the program, as well as several factors that caused TSA to miss initial deadlines for issuing TWIC cards. In our September 2006 report, we identified the challenges that TSA encountered during TWIC program testing, and several problems related to contract planning and oversight. Specifically, we reported that DHS and industry stakeholders faced difficult challenges in ensuring that biometric access control technologies will work effectively in the maritime environment where the Transportation Worker Identification Credential program is being initially tested. In October 2007, we testified that TSA had made progress in implementing the program and addressing our recommendations regarding contract planning and oversight and coordination with stakeholders. For example, TSA reported that it added staff with program and contract management expertise to help oversee the contract and developed plans for conducting public outreach and education efforts.[13] However, DHS has not yet determined how and when it will implement a biometric identification system for access controls at commercials airports. We have initiated ongoing work to further assess DHS's efforts to establish procedures for implementing biometric identifier systems for airport secured areas access control.

Aviation Security Workforce. We concluded that DHS has generally achieved all 7 performance expectations in this area. For example, TSA has hired and deployed a federal screening workforce at over 400

[11] GAO-06-597T and GAO-04-728.

[12] GAO, *Port Security: Better Planning Needed to Develop and Operate Maritime Worker Identification Card Program*, GAO-05-106 (Washington, D.C.: December 2004), and *Transportation Security: DHS Should Address Key Challenges before Implementing the Transportation Worker Identification Credential Program*, GAO-06-982 (Washington, D.C.: September 2006).

[13] GAO, *Maritime Security: The SAFE Port Act and Efforts to Secure Our Nation's Seaports*, GAO-08-86T (Washington, D.C. October 4, 2007).

commercial airports nationwide, and has developed standards for determining TSO staffing levels at airports. TSA also established numerous programs to train and test the performance of its TSO workforce, although we reported that improvements in these efforts can be made. Among other efforts, in December 2005, TSA reported completing enhanced explosives detection training for over 18,000 TSOs, and increased its use of covert testing to assess vulnerabilities of existing screening systems. TSA also established the Screening Partnership Program which allows eligible airports to apply to TSA to use a private screening workforce. In addition, TSA has trained and deployed federal air marshals on high-risk flights; established standards for training flight and cabin crews; and established a Federal Flight Deck Officer program to select, train, and allow authorized flight deck officers to use firearms to defend against any terrorist or criminal acts. Related to flight and cabin crew training, TSA revised its guidance and standards to include additional training elements required by law and improve the organization and clarity of the training. TSA also increased its efforts to measure the performance of its TSO workforce through recertification testing and other measures.

Passenger Prescreening. We reported that DHS has generally achieved one, and has not generally achieved two, of the performance expectations in this area. For example, TSA established policies and procedures to ensure that individuals known to pose, or suspected of posing, a risk or threat to security are identified and subjected to appropriate action. Specifically, TSA requires that air carriers check all passengers against the Selectee List, which identifies individuals that represent a higher than normal security risk and therefore require additional security screening, and the No Fly List, which identifies individuals who are not allowed to fly.[14] However, TSA has faced a number of challenges in developing and implementing an advanced prescreening system, known as Secure Flight, which will allow TSA to take over the matching of passenger information against the No Fly and Selectee lists from air carriers, as required by law.[15] In 2006, we reported that TSA had not conducted critical activities in accordance with best practices for large-scale information technology programs and had not followed a disciplined life cycle approach in

[14] In accordance with TSA-issued security requirements, passengers on the No Fly List are denied boarding passes and are not permitted to fly unless cleared by law enforcement officers. Similarly, passengers who are on the Selectee List are issued boarding passes, and they and their baggage undergo additional security measures.

[15] See 49 U.S.C. § 44903(j)(2)(C).

developing Secure Flight.[16] In March 2007, DHS reported that as a result of its rebaselining efforts, more effective government controls were developed to implement Secure Flight and that TSA was following a more disciplined development process. DHS further reported that it plans to begin parallel operations with the first group of domestic air carriers during fiscal year 2009 and to take over full responsibility for watch list matching in fiscal year 2010. We are continuing to assess TSA's efforts in developing and implementing the Secure Flight program. We have also reported that DHS has not yet implemented enhancements to its passenger prescreening process for passengers on international flights departing from and bound for the United States.[17] Although CBP recently issued a final rule that will require air carriers to provide passenger information to CBP prior to a flight's departure so that CBP can compare passenger information to the terrorist watch lists before a flight takes off, this requirement is not scheduled to take effect until February 2008. In addition, while DHS plans to align its international and domestic passenger prescreening programs under TSA, full implementation of an integrated system will not occur for several years.

Checkpoint Screening. We reported that DHS has generally achieved two, and has not generally achieved one, of the performance expectations in this area. For example, we reported that TSA has developed processes and procedures for screening passengers at security checkpoints and has worked to balance security needs with efficiency and customer service

[16] GAO, *Aviation Security: Management Challenges Remain for the Transportation Security Administration's Secure Flight Program*, GAO-06-864T (Washington, D.C.: June 2006).

[17] GAO, *Aviation Security: Progress Made in Systematic Planning to Guide Key Investment Decisions, but More Work Remains*, GAO-07-448T (Washington, D.C.: February 2007) and GAO, *Aviation Security: Efforts to Strengthen International Passenger Prescreening Are Under Way, but Planning and Implementation Issues Remain*, GAO-07-346 (Washington, D.C.: May 2007).

considerations.[18] More specifically, in April 2007, we reported that modifications to standard operating procedures were proposed based on the professional judgment of TSA senior-level officials and program-level staff, as well as threat information and the results of covert testing. However, we found that TSA's data collection and analyses could be improved to help TSA determine whether proposed procedures that are operationally tested would achieve their intended purpose. We also reported that DHS and its component agencies have taken steps to improve the screening of passengers to address new and emerging threats. For example, TSA established two recent initiatives intended to strengthen the passenger checkpoint screening process: (1) the Screening Passenger by Observation Technique program, which is a behavior observation and analysis program designed to provide TSA with a nonintrusive means of identifying potentially high- risk individuals; and the (2) Travel Document Checker program which replaces current travel document checkers with TSOs who have access to sensitive security information on the threats facing the aviation industry and check for fraudulent documents. However, we found that while TSA has developed and tested checkpoint technologies to address vulnerabilities that may be exploited by identified threats such as improvised explosive devices, it has not yet effectively deployed such technologies. In July 2006, TSA reported that it installed 97 explosives trace portal machines—which use puffs of air to dislodge and detect trace amounts of explosives on persons—at 37 airports. However, DHS identified problems with these machines and has halted their deployment. TSA is also developing backscatter technology, which identifies explosives, plastics and metals, giving them shape and form and allowing them to be visually interpreted.[19] However, limited progress has been made in fielding this technology at passenger screening checkpoints. The Implementing Recommendations of the 9/11 Commission Act of 2007 (9/11 Commission Act), enacted in August 2007, restates and amends a requirement that DHS issue a strategic plan for deploying explosive

[18] For more information, see GAO, Aviation Security: Risk, Experience, and Customer Concerns Drive Changes to Airline Passenger Screening Procedures, but Evaluation and Documentation of Proposed Changes Could Be Improved, GAO-07-634 (Washington, D.C.: May 2007); GAO, Aviation Security: TSA's Change to Its Prohibited Items List Has Not Resulted in Any Reported Security Incidents, but the Impact of the Change on Screening Operations Is Inconclusive, GAO-07-623R (Washington, D.C.: April 2007); GAO, Airport Passenger Screening: Preliminary Observations on Progress Made and Challenges Remaining, GAO-03-1173 (Washington, D.C.: September 2003); and GAO, Aviation Security: Enhancements Made in Passenger and Checked Baggage Screening, but Challenges Remain, GAO-06-371T (Washington, D.C.: April 2006).

[19] GAO-06-371T

detection equipment at airport checkpoints and requires DHS to expedite research and develop efforts to protect passenger aircraft from explosives devices.[20] We are currently reviewing DHS and TSA's efforts to develop, test and deploy airport checkpoint technologies.[21]

Checked Baggage Screening. We concluded that DHS has generally achieved all three performance expectations in this area. Specifically, from November 2001 through June 2006, TSA procured and installed about 1,600 Explosive Detection Systems (EDS) and about 7,200 Explosive Trace Detection (ETD) machines to screen checked baggage for explosives at over 400 commercial airports.[22] In response to mandates to field the equipment quickly and to account for limitations in airport design, TSA generally placed this equipment in a stand-alone mode—usually in airport lobbies—to conduct the primary screening of checked baggage for explosives.[23] Based in part on our previous recommendations, TSA later developed a plan to integrate EDS and ETD machines in-line with airport baggage conveyor systems. The installation of in-line systems can result in considerable savings to TSA through the reduction of TSOs needed to operate the equipment, as well as increased security. Despite delays in the widespread deployment of in-line systems due to the high upfront capital investment required, TSA is pursuing the installation of these systems and is seeking creative financing solutions to fund their deployment. In March 2007, DHS reported that it is working with airport and air carrier stakeholders to improve checked baggage screening solutions to enhance security and free up lobby space at airports. The installation of in-line baggage screening systems continues to be an issue of congressional concern. For example, the 9/11 Commission Act reiterates a requirement

[20] See Pub. L. No. 110-53, §§1607, 1610, 121 Stat. 266, 483-85 (2007).

[21] For more information, see GAO-06-371T.

[22] Explosive detection systems (EDS) use specialized X-rays to detect characteristics of explosives that may be contained in baggage as it moves along a conveyor belt. Explosive trace detection (ETD) works by detecting vapors and residues of explosives. Human operators collect samples by rubbing swabs along the interior and exterior of an object that TSOs determine to be suspicious, and place the swabs in the ETD machine, which then chemically analyzes the swabs to identify any traces of explosive materials.

[23] For more information, see GAO, *Aviation Security: TSA Oversight of Checked Baggage Screening Procedures Could Be Strengthened*, GAO-06-869 (Washington, D.C.: July 2006), GAO-06-371T, and GAO-07-448T.

that DHS submit a cost-sharing study along with a plan and schedule for implementing provisions of the study, and requires TSA to establish a prioritization schedule for airport improvement projects such as the installation of in-line baggage screening systems.[24]

Air Cargo Security. We reported that TSA has generally achieved two, and has not generally achieved one, of the performance expectations in this area. Specifically, TSA has developed a strategic plan for domestic air cargo security and has taken actions to use risk management principles to guide investment decisions related to air cargo bound for the United States from a foreign country, referred to as inbound air cargo, but these actions are not yet complete. For example, TSA plans to assess inbound air cargo vulnerabilities and critical assets—two crucial elements of a risk-based management approach—but has not yet established a methodology or time frame for how and when these assessments will be completed.[25] TSA has also developed and implemented procedures to screen domestic and inbound air cargo. We reported in October 2005 that TSA had significantly increased the number of domestic air cargo inspections conducted of air carrier and indirect air carrier compliance with security requirements. However, we also reported that TSA exempted certain cargo from random inspection because it did not view the exempted cargo as posing a significant security risk, although air cargo stakeholders noted that such exemptions may create potential security risks and vulnerabilities since shippers may know how to package their cargo to avoid inspection.[26] In part based on a recommendation we made, TSA is evaluating existing exemptions to determine whether they pose a security risk, and has removed some exemptions that were previously allowed. The 9/11 Commission Act requires, no later than 3 years after its enactment, that DHS have a system in place to screen 100 percent of cargo transported on

[24] See Pub. L. No. 110-53, § 1603-04, 121 Stat. at 480-81.

[25] For more information, see GAO, Aviation Security: Federal Action Needed to Strengthen Domestic Air Cargo Security, GAO-06-76, (Washington, D.C.: October 2005) and GAO, Aviation Security: Federal Efforts *to Secure U.S.-Bound Air Cargo Are in the Early Stages and Could Be Strengthened*, GAO-07-660 (Washington, D.C.: April 2007).

[26] GAO-06-76.

passenger aircraft.[27] Although TSA has taken action to develop plans for securing air cargo and establishing and implementing procedures to screen air cargo, DHS has not yet developed and implemented screening technologies. DHS is pursuing multiple technologies to automate the detection of explosives in the types and quantities that would cause catastrophic damage to an aircraft in flight. However, TSA acknowledged that full development of these technologies may take 5 to 7 years. In April 2007, we reported that TSA and DHS's S&T Directorate were in the early stages of evaluating and piloting available aviation security technologies to determine their applicability to the domestic air cargo environment. We further reported that although TSA anticipates completing its pilot tests by 2008, it has not yet established time frames for when it might implement these methods or technologies for the inbound air cargo system.[28]

Cross-cutting Issues Have Hindered DHS's Efforts in Implementing Its Mission and Management Functions

Our work has identified homeland security challenges that cut across DHS's mission and core management functions. These issues have impeded the department's progress since its inception and will continue as DHS moves forward. While it is important that DHS continue to work to strengthen each of its mission and core management functions, to include aviation security, it is equally important that these key issues be addressed from a comprehensive, department-wide perspective to help ensure that the department has the structure and processes in place to effectively address the threats and vulnerabilities that face the nation. These issues include: (1) transforming and integrating DHS's management functions; (2) establishing baseline performance goals and measures and engaging in effective strategic planning efforts; (3) applying and strengthening a risk management approach for implementing missions and making resource allocation decisions; (4) sharing information with key stakeholders; and (5) coordinating and partnering with federal, state and local, and private sector agencies. We have made numerous recommendations to DHS to

[27] See Pub. L. No. 110-53, § 1602, 121 Stat. at 477-79.This provision defines screening as a physical examination or non-intrusive method of assessing whether cargo poses a threat to transportation security that includes the use of technology, procedures, personnel, or other methods to provide a level of security commensurate with the level of security for the screening of passenger checked baggage. Methods such as solely performing a review of information about the contents of cargo or verifying the identity of a shipper of the cargo, including whether a known shipper is registered in TSA's known shipper database, do not constitute screening under this provision.

[28] GAO-07-660.

strengthen these efforts, and the department has made progress in implementing some of these recommendations.

DHS has faced a variety of difficulties in its efforts to transform into a fully functioning department. We designated DHS's implementation and transformation as high-risk in part because failure to effectively address this challenge could have serious consequences for our security and economy. DHS continues to face challenges in key areas, including acquisition, financial, human capital, and information technology management. This array of management and programmatic challenges continues to limit DHS's ability to effectively and efficiently carry out its mission. In addition, transparency plays an important role in helping to ensure effective and efficient transformation efforts. We have reported that DHS has not made its management or operational decisions transparent enough so that Congress can be sure it is effectively, efficiently, and economically using the billions of dollars in funding it receives annually. More specifically, in April 2007, we testified that we have encountered access issues during numerous engagements at DHS, including significant delays in obtaining requested documents that have affected our ability to do our work in a timely manner.[29] The Secretary of DHS and the Under Secretary for Management have stated their desire to work with us to resolve access issues and to provide greater transparency. It will be important for DHS and its components to become more transparent and minimize recurring delays in providing access to information on its programs and operations so that Congress, GAO, and others can independently assess its efforts.

In addition, DHS has not always implemented effective strategic planning efforts and has not yet fully developed performance measures or put into place structures to help ensure that the agency is managing for results. We have identified strategic planning as one of the critical success factors for new organizations, and reported that both DHS's and TSA's efforts in this area have been mixed. For example, with regards to TSA's efforts to secure air cargo, we reported that TSA completed an Air Cargo Strategic Plan in November 2003 that outlined a threat-based risk management approach to securing the nation's domestic air cargo system, and that this plan identified strategic objectives and priority actions for enhancing air cargo security based on risk, cost, and deadlines. However, we reported

[29] GAO, *Department of Homeland Security: Observations on GAO Access to Information on Programs and Activities*, GAO-07-700T, (Washington, D.C.: April 2007).

that TSA had not developed a similar strategy for addressing the security of inbound air cargo—cargo transported into the United States from foreign countries, including how best to partner with CBP and international air cargo stakeholders. In another example, we reported that TSA had not yet developed outcome-based performance measures for its foreign airport assessment and air carrier inspection programs, such as the percentage of security deficiencies that were addressed as a result of TSA's on-site assistance and recommendations, to identify any aspects of these programs that may need attention. We recommended that DHS direct TSA and CBP to develop a risk-based strategy, including specific goals and objectives, for securing air cargo;[30] and develop outcome-based performance measures for its foreign airport assessment and air carrier inspection programs.[31] DHS generally concurred with GAO's recommendations.

DHS has also not fully adopted and applied a risk management approach in implementing its mission and core management functions. Risk management has been widely supported by the President and Congress as an approach for allocating resources to the highest priority homeland security investments, and the Secretary of Homeland Security and the Assistant Secretary for Transportation Security have made it a centerpiece of DHS and TSA policy. Several DHS component agencies and TSA have worked towards integrating risk-based decision making into their security efforts, but we reported that these efforts can be strengthened. For example, TSA has incorporated certain risk management principles into securing air cargo, but has not completed assessments of air cargo vulnerabilities or critical assets—two crucial elements of a risk-based approach without which TSA may not be able to appropriately focus its resources on the most critical security needs. TSA has also incorporated risk-based decision making when making modifications to airport checkpoint screening procedures, to include modifying procedures based on intelligence information and vulnerabilities identified through covert testing at airport checkpoints. However, in April 2007 we reported that TSA's analyses that supported screening procedural changes could be strengthened. For example, TSA officials decided to allow passengers to

[30] GAO-07-660.

[31] GAO, *Aviation Security: Foreign Airport Assessments and Air Carrier Inspections Help Enhance Security, but Oversight of These Efforts Can Be Strengthened*, GAO-07-729 (Washington, D.C.: May 11, 2007).

carry small scissors and tools onto aircraft based on their review of threat information—which indicated that these items do not pose a high risk to the aviation system—so that TSOs could concentrate on higher threat items.[32] However, TSA officials did not conduct the analysis necessary to help them determine whether this screening change would affect TSO's ability to focus on higher-risk threats.[33]

We have further reported that opportunities exist to enhance the effectiveness of information sharing among federal agencies, state and local governments, and private sector entities. In August 2003, we reported that efforts to improve intelligence and information sharing need to be strengthened, and in 2005, we designated information sharing for homeland security as high-risk.[34] In January 2005, we reported that the nation still lacked an implemented set of government-wide policies and processes for sharing terrorism-information, but DHS has issued a strategy on how it will put in place the overall framework, policies, and architecture for sharing information with all critical partners—actions that we and others have recommended.[35] DHS has taken some steps to implement its information sharing responsibilities. States and localities are also creating their own information "fusion" centers, some with DHS support. With respect to aviation security, the importance of information sharing was recently highlighted in the 9/11 Commission Act, which requires DHS to establish a plan to promote the sharing of transportation security information among DHS and federal, state and local agencies, tribal governments, and appropriate private entities.[36] The Act also requires that DHS provide timely threat information to carriers and operators that are preparing and submitting a vulnerability assessment and

[32] GAO, *Aviation Security: Risk, Experience, and Customer Concerns*, GAO-07-634 (Washington, D.C.: May 2007).

[33] GAO, *Aviation Security: Risk, Experience, and Customer Concerns Drive Changes to Airline Passenger Screening Procedures, but Evaluation and Documentation of Proposed Changes Could Be Improved*, GAO-07-634 (Washington, D.C.: April 16, 2007).

[34] GAO, *Homeland Security: Efforts to Improve Information Sharing Need to Be Strengthened*, GAO-03-760 (Washington, D.C.: August 2003) and GAO, *HIGH- RISK SERIES: An Update GAO-05-207* (Washington, D.C.: January 2005).

[35] GAO-07-454.

[36] See Pub. L. No. 110-53, § 1203, 121 Stat. at 383-86.

security plan, including an assessment of the most likely methods that could be used by terrorists to exploit weaknesses in their security.[37]

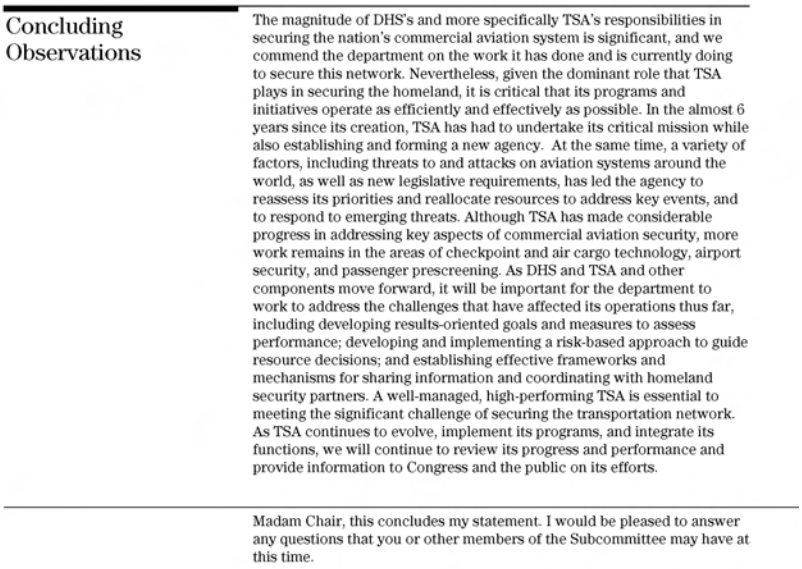
In addition to providing federal leadership with respect to homeland security, DHS also plays a large role in coordinating the activities of key stakeholders, but has faced challenges in this regard. To secure the nation, DHS must form effective and sustained partnerships between legacy component agencies and a range of other entities, including other federal agencies, state and local governments, the private and nonprofit sectors, and international partners. We have reported that successful partnering and coordination involves collaborating and consulting with stakeholders to develop and agree on goals, strategies, and roles to achieve a common purpose; identify resource needs; establish a means to operate across agency boundaries, such as compatible procedures, measures, data, and systems; and agree upon and document mechanisms to monitor, evaluate, and report to the public on the results of joint efforts.[38] We have found that the appropriate homeland security roles and responsibilities within and between the levels of government, and with the private sector, are evolving and need to be clarified. For example, we reported that opportunities exists for TSA to work with foreign governments and industry to identify best practices for securing air cargo, and recommended that TSA systematically compile and analyze information on practices used abroad to identify those that may strengthen the department's overall security efforts.[39] Further, regarding efforts to respond to in-flight security threats, which—depending on the nature of the threat—could involve 15 federal agencies and agency components, we recommended that DHS and other departments document and share their respective coordination and communication strategies and response procedures.[40]

[37] See Pub. L. No. 110-53, §§ 1512(d)(2), 1531(d)(2), 121 Stat. at 430, 455.

[38] GAO, *Homeland Security: Management and Programmatic Challenges Facing the Department of Homeland Security*, GAO-07-833T (Washington, D.C.: May 2007)

[39] GAO-07-660

[40] GAO,Aviation Security: Federal Coordination for Responding to In-flight Security Threats Has Matured, but Procedures Can Be Strengthened, GAO-07-891R (Washington, D.C.: July 31, 2007).



Ms. JACKSON LEE. Thank you very much for your insightful testimony.

It is now my pleasure to recognize Assistant Secretary Kip Hawley to summarize his statement for 5 minutes.

STATEMENT OF HON. KIP HAWLEY, ASSISTANT SECRETARY, TRANSPORTATION SECURITY ADMINISTRATION

Mr. HAWLEY. Thank you. Good afternoon, Chairwoman Jackson Lee and members of the subcommittee. It is a great pleasure to be here today to talk with you about how TSA is doing in its mission to improve aviation security. It is also a pleasure to be here to share the panel with Cathy Berrick from GAO and Frank Hatfield from the FAA.

I didn't refer to it in my submitted remarks about the ongoing, very close work that we do with the FAA, but I look forward to discussing the nature of that partnership. It is one that is very close at all levels, and I would like to publicly thank Frank Hatfield and his team for the outstanding leadership and cooperation and coordination that we do together.

I would also like to thank the committee for its continued support for our mission and your leadership in the area of improving aviation security. I particularly appreciate this committee's de-

tailed understanding of TSA's operational needs and the committee's focus on practical solutions to complex problems.

The challenges of implementing all the provisions of the 9/11 Act are formidable, but TSA is committed to achieve the objectives of this committee, the Congress and the 9/11 Commission. With all that we do, we must keep our focus on the highest priority items, priorities informed and driven by the current threat environment. Since last June, we have witnessed disrupted attacks in London, Denmark, and Germany, as well as a completed attack on Glasgow's airport in Scotland. There is no reason to think that we are exempt from that kind of attack planning.

The national intelligence estimate indicates that over the next 3 years, the threat will continue, with terrorists attempting transportation sector attacks on a grand scale. We must use our security measures that are unpredictable, agile and adaptable to put us one step ahead of evolving threats. As I have said in previous meetings with this committee, TSA has added layers of security and additional technology to our airport operations. We have continued to provide more training and real-threat testing of our frontline officers. Federal air marshals move invisibly to protect Americans wherever they fly around the globe, and VIPR teams are deployed every week in support of our shared mission with our stakeholders.

That is our focus every day. It is on that base of daily operations that we address the new requirements from the 9/11 legislation. When I was before this committee recently, we talked about Secure Flight. I promised that we would complete the re-baselining of the program, build in privacy protections, and publish the rule. We have done these things and we are ready to go.

The rule for Secure Flight has been published, and after a public hearing in September that was available live on the Internet, the comment period is open now. It closes next week and we expect to get the final rule out in spring, 2008. Should the Congress choose to fully fund the program in fiscal year 2008, we can begin testing in 2008.

I am mindful that despite the progress TSA has made across the board, much is left to do. I look forward to our work together to further strengthen security throughout our transportation network.

I look forward to the chance to discuss these issues with you. Thank you.

[The statement of Mr. Hawley follows:]

PREPARED STATEMENT OF THE HONORABLE KIP HAWLEY, ASSISTANT SECRETARY, TRANSPORTATION SECURITY

OCTOBER 16, 2007

Good afternoon Chairwoman Jackson Lee, Ranking Member Lungren, and distinguished members of the Subcommittee. Thank you for this opportunity to share with you the ongoing efforts of the Transportation Security Administration (TSA) to improve security in the aviation system by providing a better experience for travelers.

Ongoing Threat

The effort to ensure the security of the aviation system remains as important now as it ever has been in the past six years. Since August 10, 2006, the nation's threat level for all commercial aviation operating in or destined for the United States has been High, or Orange. The National Intelligence Estimate on threats to the U.S. Homeland issued in July confirmed publicly that the terrorist threat is real. This threat is persistent and evolving. Terrorists maintain an undiminished intent to at-

tack the Homeland and show a continued effort to adapt and improve their capabilities. They are innovative in overcoming security obstacles. They are training to use improvised explosive devices (IEDs). Terror groups continue to focus on prominent infrastructure targets with the goal of producing mass casualties. The aviation threat level Orange remains operationally required based on the very real threats posed by those who wish to do harm to our aviation system.

Keeping Ahead of Terrorists

TSA's security strategy is based on flexible, mobile, and unpredictable methods. To counter the evolving threat and adaptive capabilities of terrorists, we are staying ahead by rethinking the entire screening process and changing the legacy systems that originated in the 1970s. We are going on the offense to address current threats. We will be more proactive and we must anticipate the threats.

We recognize that we cannot protect every person or all property against every possible threat to the system. Given the nature of the threats to aviation, we must manage risk consistent with what we understand of the threats, vulnerabilities, and consequences. We will prioritize our resources to protect against the high-threat, high-consequence events.

I previously shared with this Subcommittee an overview of the many layers of security protecting aviation. We continue to change what we do, how we do it, and where we do it. We have significantly increased the layers of security throughout the airport environment. Risk-based security means that we share resources across all risks, both high and low, in strategic proportions.

The discussion of aviation security almost always starts at the familiar TSA security checkpoint. For the two million travelers a day who fly, that is TSA to them. However, TSA looks at the checkpoint as but a piece—an important piece—of a much larger picture. Therefore, before discussing checkpoint issues, I would like to point out that TSA looks at the entire transportation network in evaluating risk, including threat information. A large part of TSA's work involves working closely on a daily basis with the intelligence and law enforcement communities and our global partners to try to stay ahead of the current threat.

We have to be strong at the checkpoint, but also many other places—including the back, front, and sides of the airport. Risk-based security means that we take the whole picture into account and implement selective and unpredictable security measures. We must first deny the terrorist a stationary target where a planner can take the time to map an attack with high odds of success. Nothing can be uncovered, but likewise, we cannot fool ourselves into thinking that fixed, robust security is impenetrable. Our security needs to play offense, not just defense.

TSA is focusing beyond the physical checkpoint—to push our borders out, so to speak—to look more at people and to identify those with hostile intent or those conducting surveillance even if they are not carrying a prohibited item. By spreading our layers of security throughout the airport environment and elsewhere, we have multiple opportunities to detect terrorists and leverage the capabilities of our workforce, our partners, and our technology.

Travel Document Checking

We are placing specially trained Transportation Security Officers (TSOs) at the front of the checkpoint to review travel documents to find fraudulent identification (IDs) and also to look at behavior. The 9/11 Commission recognized that travel documents are akin to weapons for terrorists. We will make it harder for dangerous people to use fraudulent documents and IDs by raising the standard of inspection and providing additional equipment for our TSOs to perform this function. We ask this Subcommittee to fully support the President's budget for this program so that TSA can make a seamless transition from the airlines and continue the program with as little disruption as possible to the flow of passenger screening.

Behavior Observation

We continue to expand the Screening Passengers by Observation Techniques (SPOT) program, which utilizes non-intrusive behavior observation and analysis techniques to identify potentially high-risk passengers. Individuals exhibiting specific observable behaviors may be referred for additional screening at the checkpoint that may include handwanding, pat down, or physical inspection of their carry-on baggage. SPOT adds an element of unpredictability to the security screening process that is easy for passengers to navigate but difficult for terrorists to manipulate. It serves as an important additional layer of security in the airport environment, requires no additional specialized screening equipment, can easily be deployed to other modes of transportation, and presents yet one more challenge for terrorists attempting to defeat our security system. The SPOT program has already added great value to our overall security system. For example, a Behavior Detection Officer re-

cently identified an individual at a ticket counter carrying a loaded gun and more than 30 rounds of ammunition.

Aviation Direct Access Screening Program

We continue to expand the Aviation Direct Access Screening Program—deploying TSOs and Transportation Security Inspectors (TSIs) to locations throughout airports to screen airport employees, their accessible property, and vehicles entering a direct access point to secured areas of airports. The random screening at unexpected locations is a valuable measure to increase the protection on the "back side" of airports.

This random and unpredictable screening allows airport workers to perform their duties with minimal interruptions and keeps the aviation industry operating. TSA's approach is both practical and effective. Requiring 100% screening of all airport workers, even in a pilot program, is contrary to this philosophy; it unnecessarily diverts resources from higher risk operations without providing the improvements in security that we need. We would like to continue to work with the Subcommittee to craft a pilot program that will test varying methods of improving an airport worker screening program that will offer better security.

Bomb Appraisal Officers

We are continuing to hire and deploy Bomb Appraisal Officers (BAO) who provide advanced training for the workforce on explosives and IEDs and resolve alarms beyond the TSO capability. BAOs have extensive backgrounds and experience in IEDs as well as in Chemical, Biological, Radiological, and Nuclear threats. They work closely with local law enforcement, bomb squads, and military Explosive Ordnance Disposal personnel to satisfy TSA's explosives detection needs.

Visible Intermodal Prevention and Response Teams

Over this past summer we began to more broadly deploy Visible Intermodal Prevention and Response (VIPR) teams. Comprised of TSOs, TSIs, and Federal Air Marshals (FAMs), VIPR teams collaborate with local law enforcement agencies to intensify the visible presence of security personnel at various points throughout the transportation system. At airports, we use VIPR teams in locations away from the screening checkpoint. VIPR teams have proven that TSA and our stakeholders can greatly improve security by altering and enhancing security measures at airports.

This strategy of active, nimble, flexible security depends on the quality of the people involved. TSA has had a major focus on improving security by improving the capabilities of its people. Better recruiting and hiring, better training, better incentive systems, career progression opportunity, more involvement in decisions effecting the workforce, and more recognition of the critical role played by our people—these efforts all have a positive effect on the security result TSA delivers. The success of all these programs in increasing the layers of security would not be possible without the incredible effort, professionalism, and dedication shown by TSA's workforce. Our highly trained and highly motivated workforce—TSOs, TSIs, FAMs, and other professionals—have proven to be a nimble, adaptable workforce that can quickly adjust to counter an emerging terrorist threat. In August of 2006, TSOs employed new standard operating procedures within hours to deal with the threat identified as part of the United Kingdom plot to blow up commercial aircraft with liquid explosives. TSA has rapidly deployed FAMs to international destinations to support its mission coverage based on new threats. We are constantly reviewing and adjusting our procedures and strategies to ensure our personnel are ahead of the next threat. TSA's workforce has met every challenge in the past five years and I am confident they will continue to do so.

Maintaining a healthy, able-bodied workforce is also critical to TSA's mission. We improved workplace safety through a series of aggressive initiatives, including nurse case managers, Optimization and Safety Teams, automated injury claims filing process, involvement of the National Advisory Council in planning and implementing the Safety Week Campaign and other aspects of the Safety Program, deployment of contract safety specialists to support TSA field operations, and speedy investigations to correct safety problems. Through these programs, TSA has reduced the rate for employees losing time from duty due to injury by almost half from 11.56 per 100 employees in FY2005 to 6.75 for the 3rd Quarter of FY2007.

We are also adding significant new technology. A lesson from 9/11 is that we must be proactive—we must anticipate threats that continue to grow in sophistication and complexity. This effort includes leveraging the skills of our TSOs with new technology. This next generation of technology will assist our TSOs in separating friend from foe, increasing efficiency, and helping minimize the impact to travelers and businesses:

• *Advanced Technology (AT) X-ray.* We will begin deploying AT X-ray equipment for carry-on baggage. It provides TSOs with a better capability to identify and detect threats through improved imagery and analysis tools.
• *Checkpoint Automated Carry-On Explosives Detection Systems (Auto-EDS).* We are exploring Auto-EDS for inspecting carry-on items. Auto-EDS may provide additional detection and automation opportunities.
• *Whole Body Imagers.* We are pilot testing whole body imagers, such as the backscatter and millimeter wave technologies, to quickly and safely screen passengers for prohibited items without the need for physical contact.
• *Cast & Prosthesis Scanner.* We are testing new cast and prosthesis scanners to provide a safe, dignified, and non-invasive way to identify potential threats and clear passengers wearing casts, braces, and prosthetic devices.
• *Bottled Liquids Scanners.* We have begun deploying liquids scanning devices at checkpoints, and are now using a hand-held liquids scanner for non-checkpoint screening locations.
• *New Explosives Detection Systems.* We are evaluating several new products that will greatly increase the speed of handling and screening checked baggage, particularly when integrated into an airport's baggage handling system, while reducing the size of the footprint of the baggage screening location.

Improving Security By Improving the Security Experience

Despite the critical need for enhanced security measures, such as the requirement to remove all shoes and the restrictions on liquids, gels, and aerosols, we know we need to improve the checkpoint screening process so it is less stressful for the traveling public.

Working with our stakeholders, we are pursuing programs and processes that improve the security screening process. We are moving from the legacy approach of simply looking for weapons to a more fluid process focused on the goals of: (1) improving detection of explosives; and (2) developing the capability to evaluate travel documents as well as detect hostile intent or possible surveillance.

Looking Ahead

Implementation of Public Law 110–53, Implementing Recommendations of the 9/11 Commission Act of 2007 (9/11 Act)

TSA appreciates the leadership of this Subcommittee for the exceptionally difficult work in melding together the transportation security provisions in the Implementing Recommendations of the 9/11 Commission Act of 2007 (P. L. 110–53). I also would like to thank the Subcommittee staff for its professionalism and the hard work and cooperative spirit they displayed in working with the Department of Homeland Security and TSA to finalize these provisions.

A large proportion of the requirements in the 9/11 Act directly affect all aspects of transportation security, including strategic planning, aviation security, rail security, security of public transit facilities, pipelines, over-the-road buses, and trucking security. TSA has a big task in continuing the implementation of the 9/11 Act and in working with the many stakeholders in the transportation sector to assure the level of security that Congress and the 9/11 Commission envisioned.

We will now need to integrate the many mandates in the 9/11 Act into our current priorities and resources to enable key initiatives to progress without delay while not losing focus on our threat-based operations. I also ask the Subcommittee to recognize that many of the mandates propose implementation schedules that will be especially challenging, given requirements in other laws for sufficient time to allow the Federal regulatory process to fully play out. We are working with our partners in the Department and other federal agencies to begin this process and will report our progress at the request of the Subcommittee.

Screening of Air Cargo

As you know, the 9/11 Act requires the establishment of a system to screen 100 percent of cargo transported on passenger aircraft within 3 years. As we proceed towards meeting the cargo screening requirement, TSA will stress effective security management of the air cargo supply chain. This process will require substantial collaboration with stakeholders. This Subcommittee was a leader in including key language in the bill that authorizes TSA to develop and implement a process to certify the security methods used by shippers as a means of complying with the screening requirement. This is a critical element in enabling the improved security for air cargo on passenger aircraft that Congress requires. I am grateful to the Committee for its recognition that better screening occurs when shipments are screened and secured at various points along the supply chain. Waiting until the freight is dropped at the airport, often in large pallets, to begin screening would result in less effective screening as well as defeat the whole purpose of the air cargo system that strives

to provide expeditious delivery of goods from origin to destination. We expect to work closely with all aspects of the air cargo supply chain to develop an effective and robust air cargo security program in accordance with the bill's requirements while continuing the free flow of commerce that our economy relies upon. TSA will build upon our established programs: air cargo security regulations; Security Directives; the Known Shipper Management System; and increased use of TSA-certified explosives detection canine teams and Transportation Security Inspectors for Cargo.

In addition, the $80 million dollars appropriated to TSA this year for air cargo security as part of the FY2007 Emergency Supplemental Appropriations Act (P.L. 110–28) will contribute to our increased efforts through the hiring of at least 150 additional cargo inspectors and expansion of the National Explosives Detection Canine Program by no fewer than 170 teams.

Secure Flight

TSA has taken a significant step toward implementing the recommendation of the 9/11 Commission and the requirement of the Intelligence Reform and Terrorism Prevention Act of 2004 to enhance the vetting of aviation passengers against terrorist watch lists. On August 23, 2007, TSA published a Notice of Proposed Rulemaking (NPRM) proposing implementation of the Secure Flight program. Secure Flight, if implemented as proposed, will bring the process of comparing passenger names against the watch list, now performed by aircraft operators, into the government, and will align domestic and international passenger pre-screening. By establishing a more consistent and effective watch list matching process, TSA will strengthen a key layer of security and enhance its ability to stop terrorists from being allowed through the passenger screening checkpoint. The program is designed to better focus enhanced passenger screening efforts on individuals likely to pose a threat to civil aviation, and to facilitate the secure and efficient travel of the vast majority of the traveling public by distinguishing them from individuals on the watch list.

We have taken the time to build the Secure Flight program right, and we believe that the NPRM and associated Privacy Act System of Records Notice and Privacy Impact Assessment demonstrate that TSA has built a program with the operational requirements necessary to enhance aviation security while protecting the privacy and civil liberties of the traveling public.

Over the next few months, TSA intends to begin a testing period using data from aircraft operators that volunteer to participate. During testing, air carriers will continue conducting watch list checks for domestic flights, and TSA will compare the results of its watch list matching with air carrier results to ensure the validity of the Secure Flight system.

It is therefore extremely critical that Congress provide the necessary funding for Secure Flight requested by the President in the FY 2008 budget. Without the necessary funding, the program will have to scale back benchmark testing with airlines, Secure Flight system to airline system testing, parallel operations with airlines, and the stand up of the Secure Flight Service Center or Secure Flight Operations Center. In short, the program would have a system with no ability to connect, communicate, or test with airlines for the purposes of implementation. Important contract awards would be postponed. From a schedule perspective, rollout of the Secure Flight program would be severely delayed. An immediate concern is the significant budget constraint imposed on the Secure Flight program due to the enactment of H.J. Res 52, providing for continuing appropriations for fiscal year (FY)2008. The restrictions on funding under H.J. Res 52 will inhibit TSA's ability to implement this critical program to improve aviation security and fulfill a key recommendation of the 9/11 Commission. Now that we have demonstrated major progress on the Secure Flight program through the issuance of the NPRM and associated privacy documents, we need your support to fund this vital program.

General Aviation

TSA is working closely with the general aviation (GA) community to develop reasonable, feasible, and effective security for GA operations while ensuring that these measures support continued operations and increased growth of the industry.

TSA is also working with aircraft operators and Fixed Base Operators directly to develop voluntary programs of verifying the identification of passengers on board aircraft and maintaining facility security in and around GA aircraft. TSA is working closely with our interagency partners to improve GA security. The U.S. Customs and Border Protection (CBP) recently issued a NPRM that will require GA operators to submit comprehensive manifest data about passengers, crew, and flight information electronically to CBP, as part of its Electronic Advance Passenger Information System (e–APIS), at least 60 minutes before the aircraft departs for the United States.

Currently, we only receive very basic information from GA aircraft coming into the United States, such as who is and is not a U.S. citizen. That is not enough. Having this information an hour before departure will give CBP inspectors more time to fully pre-screen travelers and crews and take necessary actions to resolve threats.

Conclusion

Although the threats and challenges to the security of the aviation system are numerous, so are the solutions and efforts of TSA to continue to successfully carry out our mission. We will continue to use our personnel, information, and technology in innovative ways to stay ahead of the evolving threats and facilitate passenger travel and the flow of commerce.

Finally, I want to take this opportunity to thank the traveling public and our stakeholders for their continued cooperation which helps TSA effectively manage high travel volumes through the screening process. I am hopeful that the same level of cooperation from the traveling public and our stakeholders will make the upcoming holiday travel season a success as well. TSA has shown that in partnership with our stakeholders we can implement enhanced flexible security measures while maintaining the flow of passenger and baggage screening.

Madam Chairwoman, thank you again for the opportunity to testify today. I am happy to respond to the Subcommittee's questions.

Ms. JACKSON LEE. Assistant Secretary Hawley, thank you for your testimony as well.

I now recognize Director Franklin Hatfield to summarize his statement for 5 minutes.

STATEMENT FRANKLIN HATFIELD, DIRECTOR, SYSTEM OPERATIONS SECURITY OFFICE, FEDERAL AVIATION ADMINISTRATION

Mr. HATFIELD. Thank you, Chairwoman Jackson Lee, Congressman Lungren, members of the subcommittee. I am pleased to appear before you this afternoon to discuss the role of the FAA in supporting the Transportation Security Administration's response to aviation security threats and incidents.

I want to assure the subcommittee that FAA and TSA are aligned and work very closely together in terms of understanding and implementing our respective roles in responding to aviation security threats. The FAA supports TSA through a broad range of standing mechanisms, some of which are continuous in nature and some of which are activated in response to a specific incident.

We agree with the chairwoman's assessment that FAA's primary mission is aviation safety and efficiency, but we also agree with the chairwoman's assessment that our support of TSA's security role is equally important.

Accordingly, we work with TSA, the Department of Defense, and other key partners to effectively respond to any potential threat without compromising the safety of the national airspace system, and while attempting to mitigate the impacts on the system's efficiency. In the aftermath of 9/11, the FAA established the domestic events network, a continuous 24-hour-a-day communication capability that includes over 100 agency partners. Through the DEN, agencies monitor ongoing activity in the national airspace system, along with their respective areas of expertise, to identify anomalies to determine whether they could pose a threat, and to coordinate operational responses to defeat any such threats.

It is our first line of defense that provides ongoing information-sharing on a real-time basis. For example, FAA manages day-to-day operations of the national airspace system. Based on information provided by our air traffic controllers, our security watch offi-

cer may use the DEN to alert TSA and other partner agencies about aircraft that are flying where they shouldn't be, or aircraft that are not responding to controllers' attempts to contact them.

In the vast majority of cases, the identified aircraft turned out not to be a security threat, but providing this early information via the DEN gives our other partners in the government the opportunity to input their area of expertise in order to provide a more complete picture of what may or may not be happening. The level of interest a flight receives would obviously be determined through shared information about the situation, triggering higher levels of scrutiny as appropriate.

In addition to the DEN, the FAA supports the TSA in a variety of operational elements, including a newly named Freedom Center out in Herndon, Virginia. The Freedom Center is staffed with TSA personnel as well as representatives from various federal agencies, including the FAA, and we have air traffic controllers assigned to the facility's National Capital Region Coordination Center at the Freedom Center. If an incident arises, FAA personnel are immediately available to provide their expertise.

In addition, should the situation warrant, TSA activates a telephone bridge with ranking officials throughout DHS. This permits DHS to make quick, comprehensive, decisive decisions about a particular security threat. Usually—and I say "usually," and it is almost always—as soon as that bridge is activated, the FAA administrator's representative, myself, will immediately be joined in the network discussion. In this manner, the merits of different options can be discussed and informed decisions made and implementation of those decisions can be done expeditiously. This means of communication has been very effective, and we will talk probably more about that a little bit later on.

We also exchange technology with one another. The FAA supports TSA through this shared technology. For example, FAA provided the traffic situational display, the TSD, at key facilities operated by TSA and other partners. While TSD was designed by the FAA as an air traffic management tool, the system's ability to share situational information reduces the potential for miscommunication between our two agencies, and enhances our ability to make a rapid decision in a crisis situation.

We are actively working with TSA now and in the short term and in the long term on new technological platforms which will support TSA's aviation security responsibilities. We are also cooperating with TSA on longer-range plans for the FAA's Joint Planning and Development Office, which is currently working to integrate security capabilities into the architecture for the next generation air transportation system.

Finally, FAA and TSA partner on all the special events, most recently the United Nations General Assembly, the Super Bowl, and the upcoming World Series. These are just a few examples of the many ongoing interagency efforts designed to optimize our nation's security.

In conclusion, the FAA is committed to supporting fully TSA in its efforts to improve aviation security. While we continually look to refine and improve these efforts, I am confident that both agencies agree that our working relationship is a strong one.

This is the conclusion of my prepared statement. I will be happy to answer questions at this time. Thank you.

[The statement of Mr. Hatfield follows:]

PREPARED STATEMENT OF FRANKLIN HATFIELD

OCTOBER 16, 2007

Chairwoman Jackson-Lee, Congressman Lungren, Members of the Subcommittee:I am pleased to appear before you this afternoon to discuss the role of the Federal Aviation Administration (FAA) in supporting the Transportation Security Administration's (TSA) response to aviation security threats and incidents. I want to assure the Subcommittee that FAA and TSA are aligned and work very closely together in terms of understanding and implementing our respective roles in responding to aviation security threats. The FAA supports TSA through a broad range of standing mechanisms, some of which are continuous in nature, and some of which are activated in response to an identified threat. FAA's mission is aviation safety and efficiency. FAA supports TSA's aviation security mission. Accordingly, we work with TSA, the Department of Defense (DoD), and other key partners to effectively respond to any potential threat without compromising the safety of the National Airspace System (the NAS) and while mitigating impacts of system efficiency.

The FAA is uniquely qualified, trained, and equipped to operate the NAS and manage the nation's airspace. This is why FAA retains control of the airspace, even when security incidents arise. While other entities have missions and skill sets that are essential to responding to security threats, the FAA's understanding of the complexity of the NAS makes it uniquely suited to recognizing aviation threats and identifying the options available based on the facts of a given situation without compromising operational safety and unduly impacting NAS efficiency and the nation's economy.

As security has become a greater focus of managing air traffic, and responsibility for transportation security rests with the Department of Homeland Security (DHS), it is helpful to understand the legislative history of why the FAA was given and retains operational control of the airspace. The FAA was created almost 50 years ago in 1958 to provide a centralized focus for aviation, replacing an ineffective system of diffused authorities that had evolved over time. Prior to 1958, the functions of the FAA were splintered, with the Civil Aeronautics Authority (under the Department of Commerce) possessing day-to-day air traffic control responsibilities; the Civil Aeronautics Board possessing accident investigation and safety regulatory responsibilities; and an Airways Modernization Board having the responsibility for planning and developing a system of air navigation facilities. On top of that, there was an inter-agency Air Coordinating Committee which reviewed all matters involving use of the airspace. This approach to managing the NAS was clearly inefficient and ineffectual.

The legislative history of the Federal Aviation Act of 1958 (FAAct) makes it clear that Congress wanted one independent agency with "plenary authority" over the nation's airspace. The FAA Act was intended to address two fundamental deficiencies in the Federal Government's aviation responsibilities, one of which was a "lack of clear statutory authority for centralized airspace management." When it was unclear which civilian agency or the military had authority over air traffic, airspace and other aviation safety issues, the confusion led to aviation accidents, including mid-air collisions. The current statutory framework for the Administrator's airspace authority and the accompanying legislative history confirm that the FAA continues to be the sole authority for airspace management, air traffic regulatory authority, and use of the airspace.

To more fully understand how FAA supports the security responsibilities of the TSA and other agencies on a daily basis and in response to a perceived threat, I will review the communications and technological initiatives that are currently in place and how they work. I will also briefly summarize the ongoing government exercises to ensure that all the requisite individuals throughout government know what is expected of them should a crisis arise.

Communications

In the aftermath of 9/11, the FAA established the Domestic Events Network (DEN)—a continuous, twenty-four hour a communications capability that includes over a hundred agency partners. Through the DEN, agencies monitor ongoing activity in the National Airspace System (NAS) along with their respective areas of expertise to identify anomalies to determine whether they could pose a threat and to coordinate operational responses to defeat any such threats. The DEN enables all

of the key aviation security stakeholders to connect the dots and ensure that responses reflect the risk-based decisions of the Government. It is a first line of defense that provides ongoing information sharing on a real-time basis. For example, FAA manages day-to-day operations in the NAS. Based on information provided by controllers, our watch officer may use the DEN to alert TSA and other partners about aircraft that are flying where they shouldn't be or aircraft that are not responding to controllers' attempts to contact them. In the vast majority of cases, the identified aircraft turn out not to be a security threat, but providing early information to the DEN gives other parts of the government the opportunity to input their areas of expertise in order to provide a more complete picture of what may or may not be happening. The level of interest a flight receives would obviously be determined through shared information about the situation, triggering higher levels of scrutiny as appropriate.

In addition to the DEN, the FAA supports the TSA in a variety of operational elements, including the Freedom Center (formerly known as the Transportation Security Operations Center (TSOC)) in Herndon, Virginia. The Freedom Center is staffed with TSA personnel as well as representatives from various partner agencies, including the FAA, which has air traffic control specialists assigned to the facility's National Capital Region Coordination Center (NCRCC). If an incident arises, the FAA personnel are immediately available to provide air navigation services related input to the interagency response decisions, including information on flight behavior (e.g., flight path and communication with air traffic control (ATC)); aircraft registration; pilot history; and critical safety factors such as the FAA's ability to safely divert the aircraft to alternate landing locations while mitigating potential threats. These personnel also are able to leverage the FAA's ATC capabilities to communicate with the suspect flight and provide security driven instructions.

Should the situation warrant, TSA can activate a bridge telephone conversation with high ranking officials throughout DHS. This will permit DHS senior officials to immediately understand the situation at hand in order to make informed, coordinated decisions from the top for their immediate implementation. Usually, if this bridge is activated, the FAA Administrator's representative will immediately be joined to the network discussion. In this manner, the merits of different options can be discussed, informed decisions can be made, and implementation of those decisions can occur expeditiously.

It is important to understand that the range of potential scenarios that may unfold means that a standard protocol or checklist is neither and optimal or practical solution. When a problem is identified, the facts of any given situation will dictate how the situation is handled and what decisions get made. For example, if it is discovered that a passenger enroute to the United States is on the no-fly list, the decision of where and/or whether to divert the flight could be impacted by the actions of the passenger in question. Is the passenger exhibiting signs of anxiety or restlessness? Or is the passenger sound asleep? The specific facts around the situation could lead to different conclusions, different decisions and consequently, different results. The important thing is that the conclusions and decisions are made at the appropriate level of government with all the players in the decision making process basing those decisions on the same coordinated, integrated, real-time information.

These means of communicating have proven to be very effective in ensuring the level of response is appropriate to the threat at hand, while avoiding unduly impacting the nation's aviation system, which is already the most complex and busy system in the world, and creating unwanted economic consequences.

Technology

In addition to effective inter-agency communication, new and better technology is also an essential tool in the war against terror. The FAA supports TSA through sharing technology. For example, FAA provides the Traffic Station Display (TSD) system at key facilities operated by TSA and other partners. While TSD was only designed to support air traffic management activities, the system's ability to share situational information reduced the potential for miscommunication or misunderstanding among agencies sharing information, which, past incidents have demonstrated, is essential in reacting to developing situations appropriately.

We are actively working with TSA now both in the short and long term on new, shared and interoperable technological platforms, which will support TSA's aviation security responsibilities. We are also cooperating with TSA on longer range plans through the FAA's Joint Planning and Development Office (JPDO), which is currently working to integrate security capabilities into the architecture for the Next Generation Air Transportation System (NextGen).

Joint Planning/Coordination Groups

The FAA and TSA also work in close partnership through a variety of interagency planning groups. For example, the FAA and TSA co-chair an interagency airspace procedures working group that meets every week to discuss, resolve and ensure that positive communication and coordination continues between all agencies. We co-chair an interagency working group working on improving the Government's ability to counter and respond to Man Portable Air Defense System (MANPADS) threats posed by terrorists. We partner on event specific task forces such as those established to protect National Special Security Events (NSSE) such as the recent UN General Assembly. These are just a few examples of the many ongoing inter-agency efforts designed to optimize our nation's security.

Exercises

Improved communication and technology is further enhanced by regular joint TSA–FAA as well as national level, Government wide exercises. These exercises, which are built around various threat scenarios identified by the Intelligence Community and/or real world events (e.g., the August 2006 UK terror plot), enable the FAA and TSA to explore and refine our cooperation at all levels ranging from policy decisions to tactical operations. The FAA and TSA senior officials regularly conduct exercises led by each agency's Administrators. The last such exercise, held earlier this year in April, enabled us to explore and significantly clarify how we would work together to effectively respond to a terrorist attack premised on the UK plot scenario, in which the terrorists intended to blow up flights from Heathrow bound for the U.S.

In addition to these bilateral exercises, we participate in partnership with TSA in broader, Government wide exercises such as Top Officials 4 (TOPOFF 4), which is being conducted this week. TOPOFF 4 will help the participating agencies identify gaps and strengthen cooperation on responses to terrorist attacks using Radiological Dispersal Devices (RDD) or "dirty bombs".

In conclusion, the FAA is committed to supporting fully TSA in its efforts to improve aviation security. While we continually look to refine and improve these efforts, I am confident that both agencies agree that our working relationship is a strong one.

This is the conclusion of my prepared statement. I will be happy to answer your questions at this time.

Ms. JACKSON LEE. Let me thank you, director, for your forthrightness, and really setting the tone for this hearing. I think as I look at Assistant Secretary Hawley, and I think he lit up when he said "sharing situational information," which is key to all of our security.

At this time, I will remind each member that he or she will have 5 minutes to question the panel.

I now recognize myself for such questions, and as I do so, let me ask unanimous consent to place into the record several articles, "The FAA Alerted on al-Qa'ida in 1998, 9/11 Panel Said," and that is dated September 14, 2005; "Air Traffic Cell Towers: FAA Centers Communication Breakdown Should Worry Congress," October 14, 2007; and then "Flyers Beware, 2007 Said to be Worse Year for Delays, Report Says," September 26, 2007. Without objection so ordered.[1]

[See committee file.]

Ms. JACKSON LEE. Some would ask why I would raise these questions. As I listened to the director from GAO, I heard a 70 percent compliance. I think it is important to first thank my subcommittee members because as fast as we can review and schedule hearings, we are attempting to be broad-based in our oversight over transportation modes, and we are methodically making our way through a number of transportation modes.

Of course, aviation seems to draw the bounty of attention. But this is the reason why, and I will just read this: "According to the 9/11 panel, the American aviation officials were warned as early as 1998 that al-Qai'da could seek to hijack a commercial jet and slam

it into a U.S. landmark, according to previously secret portions of a report." Those aviation officials were the FAA.

And so, we have a calamity of occurrences here, and I think Director Hatfield made it very clear. We certainly didn't have situational exchanges prior to 9/11 in an effective manner, and I question whether or not we have situational exchanges now. I hope as we proceed in this hearing, I will be able to highlight for the record really the crisis in air traffic controllers, both in terms of personnel and equipment. This is a hearing to reflect on information, and I have already stated that I believe that the committees are certainly attempting to work together—TI and the Homeland Security. We recognize that we have joint responsibilities.

So my questions are not in any way to undermine jurisdictional territories. But it is important—I can't seem to grab enough of the vocabulary—to speak to the need for coordination between TSA and FAA, and to really highlight that when there is a breakdown in an FAA tower—Memphis Center was the one that was referred to, and FAA controllers had to use cell phones—the security of America is in jeopardy.

So I want to first begin with that focus between Director Hatfield and Assistant Secretary Hawley. That is, what is the status of situational exchange? What impact between the two agencies, TSA and FAA—what is the impact of what I think is an infrastructure problem, an upgrade problem for air traffic controllers as it relates to security? What kind of technology, what do we need to put in place to improve situational exchange and better exchange so that the pictorial scene that many of us saw in the movie that depicted 9/11, when there was certainly great heart shown by the air traffic controllers, but there was also great confusion, can projecting into the future be solved?

Director Hawley?

Mr. HAWLEY. Yes, I think first of all the real-time communication is extraordinary, as Mr. Hatfield mentioned. There are FAA air traffic experts at the Freedom Center, which is TSA's operations center. We have a variety of formal mechanisms and informal mechanisms that go up and down the chain. I think one of the most important things to mention is that we have shared intelligence analysis sessions at which Mr. Hatfield is invited, along with the administrator and deputy administrator of the FAA, with me and my deputy to go over all the intel at the highest classification level to make sure that we are all on the same page, so that if something happens, we don't have to explain what is going on; that we maintain real-time awareness on the intel front, and then we back that up with a real-time conversation when something is happening.

It is a well-practiced thing. We do formal drills, but we do so many real world situations that overlap security and safety. For instance, if we have a security concern about a flight and we are interested in a particular routing, Mr. Hatfield with the FAA will think about weather, will think about fuel load, will think about impact on air traffic in that area. And the two really have to go hand in hand, and we have to have the same information and real-time communications. I think that is the case.

Ms. JACKSON LEE. I am going to suspend and recess, and it is in the middle of my question—Mr. Hatfield, you have not answered, and Ms. Berrick—so that members could go vote. There are a series of votes. Rather than go until the end, we will suspend and the committee will be in recess, and we will be back. We apologize to the witnesses, and I will continue to hear from you, Mr. Hatfield and Ms. Berrick.

The hearing is in recess.

[Recess.]

Ms. JACKSON LEE. The hearing will now come to order. Thank you.

Mr. Hatfield, if you remember, in your testimony you mentioned the situational exchange. Mr. Hawley has indicated that there are some preliminary systems in place. I want to be more pointed. I think we are owed a great deal more affirmation and, if you will, detail in this idea of exchanges. So in your response, you might want to respond how the FAA is working with TSA in terms of the situational exchanges, which I think are very important. I would also like you to answer this question of the existence of infrastructure and the level of sophistication of that infrastructure with respect to air traffic controllers that relates to security.

Mr. HATFIELD. Okay, certainly. As I said in my opening statement, TSA and FAA work very closely together. Let me address that to begin with. In my 40 years as an air traffic controller both in the military and the FAA, the primary problem when you encounter a security issue is the common situational awareness with those other people you are trying to talk to.

On September 11, 2001, I was in New York City as the Air Traffic Division Manager for the entire east coast. During those first few hours, our major problem was trying to figure out what it was we were dealing with. And then when we thought we had an idea, reaching out to the Department of Defense or another government agency, and then trying to share with them our thoughts, and then even to find a way to be talking about the same thing.

So on that morning, a telephone conversation began. It started out with me from eastern region to the FAA headquarters telling them what was occurring in New York, what my thoughts were, where we were tracking planes, what we thought the situation was. We slowly added other FAA facilities around the country to that. So after about 1 hour, almost all of the FAA was hooked up. But it became apparent that there were other people that had a different perspective on what was occurring, specifically the Department of Defense. So we said, let's pull the Department of Defense up on this telcon with us, from a security perspective, terrorism, obviously the FBI; let's pull the FBI up.

In essence, chairwoman, that telephone has not been hung up since September 11. It has been formalized in the domestic events network. It is 24/7. There are over 100 government agencies continuously that monitor that telcon from an aviation perspective, everyone from the Pentagon police force to the Capitol police, 100 government entities.

As a direct result of that real-time instantaneous communication, let me give you a scenario. A scenario might be that Albuquerque Center calls us up and says, "Hey, we are no longer talking to

United 123, and he is deviating off-course." Instantaneously, the TSA watch-stander says, "All right, let me give you what information we have on that particular airplane." The Department of Defense says, "We are going to put some jets at runway alert right now."

So all of the various elements in the federal government are talking about the same airplane, the same place in time, with the same identical information. To me, that is the biggest step forward that we have taken in security since September 11.

Ms. JACKSON LEE. My time is far spent. Let me just quickly have a quick question. Did you act quick enough on 9/11 and are you acting quicker now?

Mr. HATFIELD. It is very difficult for me to judge. Did we act quick enough or not quick enough? Did we act quicker than anyone would ever have expected us to? That, to me, is something that it would be very difficult for me to quantify. But I can absolutely say, we are acting light-years quicker today than we were on that day and time.

Ms. JACKSON LEE. Well, let me let you think about it.

Ms. Berrick, what do you think about this situational exchange, and if you have any reflection on the 9/11 question, or more importantly the technology, and where we are today with the air traffic overload that seem to have?

Ms. BERRICK. Sure. With respect to technology, we haven't looked at that particular piece, but we did look at situational awareness and how TSA and FAA and a lot of other agencies and departments work together when there are security threats onboard an aircraft while it is in flight. Generally, we found that the coordination worked very well. The agencies were communicating. The DEN network has been up and running since 9/11.

We found a couple of issues where we made recommendations. They were related to the agencies' having policies and procedures for coordination, because although coordination was working well, a lot of it was based on the individuals that were in place. They knew each other. They knew how to work together and to communicate, but not all of the agencies had documented these procedures down so if somebody new came in, it would be apparent how to act in certain situations. So we had recommendations that agencies document and share these procedures.

And also related to exercises, that the agencies have in place exercises where they go through different scenarios and talk about how they would deal with these different scenarios, which is very positive and we said that that was a very good step. It was follow up from some of these exercises that we felt more could be done in terms of the agencies' identifying what the action items were and actually following up on those.

But overall, we found that coordination worked very well.

Ms. JACKSON LEE. I will follow up with you. I thank you.

Let me acknowledge the presence of Mr. Markey of Massachusetts.

And now let me yield to Ms. Clarke, a member of the committee, at this time for 5 minutes.

Ms. CLARKE. Thank you very much, Madam Chair.

I want to direct my questions to Assistant Secretary Hawley. It is good to see you back here again. I probably boast of one of the most diverse districts in the country. My home of Brooklyn, New York contains more people from more countries than just about anywhere else in America. This means, of course, that many of my constituents travel frequently, making great use of New York's busy airports.

When I travel home each weekend, one of the complaints about travel which I hear most is that many people are routinely delayed or detained each time they try to fly. Earlier this year, the department initiated a DHS TRIP program, in part to address these exact types of complaints.

Can you let me know whether TSA has been able to successfully transition into using this new program from previously having run its own redress process within the agency? And was it difficult for TSA employees to transition to the new system?

Mr. HAWLEY. It is actually a very smooth transition in that we are using the same technology for DHS TRIP as we have for TSA Redress. So the process is very similar. The key point that you raise is that regular travelers who have names similar to those on a watch list are sometimes inconvenienced when they try to check in, say, at home or at a kiosk.

The solution to that is the Secure Flight program that I mentioned in my opening. When that comes into place and takes the watch list matching inside the government, that problem should virtually go away. Until that time, we do depend on the airlines' systems to be able to say, "That is the person who went through DHS TRIP." So we provide that information to the airlines, but the issue is for the airline to be able to use that in its boarding process.

Ms. CLARKE. Has using DHS TRIP helped improve the efficiency of security screeners at airports, allowing officials to spend less time on misidentifications and more time looking for actual problems?

Mr. HAWLEY. I think it has definitely helped with passengers who have one face to DHS—I came into the country, and was that a Customs and Border Protection issue or was it a TSA issue? So now there is just one place to go. To the extent that we resolve the issues up front, it saves everybody time—customer, airline, and TSA. So the ultimate answer is Secure Flight.

Ms. CLARKE. So since the implementation of DHS TRIP, have you noticed any improvement in the overall travel experience for passengers? If so, has TSA done any analysis on this? Or do you have any anecdotal evidence?

Mr. HAWLEY. I think it clearly has helped a number of people, but it is too sporadic for me to really say it solved the problem. It is an effort to communicate with the public to make it easier for us to do what we can with the current system, but honestly, until we fix the system and get Secure Flight in place, it will be patchy at best. Some airlines are able to manage it quickly; others, it is more of a challenge.

Ms. CLARKE. And TSA has probably the most experience with the DHS TRIP of any agency within the department. Based on your experience, has TSA benefited overall from using DHS TRIP? And do you feel that other government agencies outside of DHS that rou-

tinely perform screening of the public could benefit from this or similar programs?

Mr. HAWLEY. Yes, I think that is a very good point, that with the visibility of watch list programs, that it is important to the public to be able to quickly resolve misidentifications. I think the idea of one-stop shopping is an excellent idea and we certainly have learned from that.

Ms. CLARKE. Thank you.

Ms. Berrick, do you feel DHS has benefited from DHS TRIP? And is it a program from which other government screening agencies outside of DHS could benefit?

Ms. BERRICK. We actually are looking at that right now as a part of the 9/11 mandate. GAO was asked to look at how Secure Flight, using their redress process, how that is working and will they be able to quickly correct misidentified and recognize misidentified passengers. So we don't have any conclusions yet. We will be reporting on this in January of 2008.

Ms. CLARKE. Thank you very much.

Thank you very much, Madam Chair.

Ms. JACKSON LEE. Let me yield now to the distinguished member from New Jersey, Mr. Pascrell, and a beloved former member of this committee.

Mr. PASCRELL. Thank you, Chairwoman Jackson Lee. It is great to be back. Thank you for letting me sit in on this subcommittee, which I am not officially a part of.

While I was away from this committee, Madam Chairwoman, in January we put our heads together and wrote a letter, drafted a letter to Mr. Hawley, the assistant secretary for TSA. We expressed our deep concern about a number of administrative failings and security vulnerabilities at Newark Airport.

Among those concerns were a series of articles that were written in the Star–Ledger, including a report on October 27, 2006 that showed failure by TSA screeners in 20 of 22 screening tests—that is interesting, I have to read things in the paper to find out what is going on these days—as well as violations of standard operating procedures. In the letter, we asked a series of questions about: Have you been able to determine the causes for the poor performance at Newark?; Were the policies and protocols followed at Newark?; Have subsequent covert tests at Newark indicated any changes in the level of performance?

You sent a response back to that letter in March, addressed to me, "Dear Congressman Pascrell," et cetera. Your response did not really address your answer to any of these very specific questions. So I would ask that you answer this committee about TSA's response to this issue in regards to these questions which were asked. That is my first question.

My second question will be on the subject of whistleblowing protection.

Mr. Hawley?

Mr. HAWLEY. Yes, sir. On the covert testing results, we have done classified briefings on those, and would be happy to do one for you as well. That is the forum to discuss the specific issues.

Mr. PASCRELL. You don't think the public has a right to know at least some very basic principles about the findings at any par-

ticular airport? Why must everything be the subject of classified information? If it was classified, and if I found it in the past to be classified, I could find some level of agreement. I do not. I think the public needs to know, has a right to know what is going on in any airport in this country. Don't you agree with that?

Mr. HAWLEY. I think on the policy level, yes. As to specific vulnerabilities, no. However, I think the points raised are good ones. Let me address them without getting into the classified part.

Mr. PASCRELL. Sure.

Mr. HAWLEY. We fundamentally changed the way we look for improvised explosive devices. We moved from training and testing of completely assembled bombs, which are a lot easier to find, to go down to the small component parts which are, for instance, like detonators that would be the size of my pen cap. So we went to a much, much, much more difficult regime of training and testing. And then we have since then deployed 5,800 of our covert testing kits. We literally have 2,500 tests a day, covert tests a day, 2,500 a day. In that, we look to see how we can challenge the system. We use people from the inside of the system who know its vulnerabilities, to test it and probe it and use it as a training example.

So I do not have a problem. If the results were the ones that you describe—and I am not going to confirm or deny that—but if they were accurate, it would be evidence of the covert testing program. When you get to the whistleblower thing, I think it raises another very important point, which is we need to be open and transparent with our workforce about our failings, about our vulnerabilities, so we can fix them. And if there is a concern about harassment or intimidation up the chain of command, that is a security issue because it covers up things that you need to know about.

Mr. PASCRELL. Before you answer the second question, very briefly, are you saying that there have been since the first tests in 2006, there have been similar screening tests of employees at the Newark Airport, and you have results of those tests?

Mr. HAWLEY. I don't know specifically. I know they are doing these covert tests that I just mentioned today at Newark and every day.

Mr. PASCRELL. Okay. I want to get to the second part. Thank you.

The report of screening failures at Newark Airport include the troubling news the Newark Airport personnel, including TSOs, the officers there, were interrogated by federal agents who were investigating the source of these leaked test results that reflected poor performance by the Newark screening staff in 2006. My impression at that time was they were more concerned about the whistleblowers than the deficiencies. That was my perception. I could be wrong. Right, Mr. Hawley? Or I could be right.

Mr. HAWLEY. Both are possible. Yes, sir.

Mr. PASCRELL. Both possible. Okay.

These screeners and security personnel are our first line of defense against terrorism. They are the people on the ground who witness first-hand every day the implementation of the security procedures we put in place. Their observations, the information we gather from them can be an invaluable resource. But it seems clear

that TSA is more interested in silencing them in the interests of not being embarrassed, than they were in listening to their own employees.

Just today in the Star–Ledger, in an entitled editorial, "Give Airport Screeners Whistleblower Protection," they cited very specific examples—Air Marshal Robert MacLean, very specific examples in this editorial brought forth by a reporter, Ron Marsico from the Star-Ledger. It would seem to me, don't you think they should be protected? Don't you think employees should be protected?

Mr. HAWLEY. Yes, no question.

Mr. PASCRELL. How are we going to get to that point?

Mr. HAWLEY. We have those protections today. They are slightly different than under the Whistleblower Protection Act. I believe we said before Congress in other situations that we would not oppose changing to the other system. I agree wholeheartedly with the premise of your question, which is workplace intimidation, particularly in the security field, is a sickness, a vulnerability, and has to be stopped.

Mr. PASCRELL. So we have come a long way in the last few months, then, in implementing this.

Mr. HAWLEY. No. I think the issue is that if it is classified information that is given out publicly, that kicks it into a different realm in terms of investigation than merely a so-called "leak."

Mr. PASCRELL. Are you familiar with the Robert MacLean case?

Mr. HAWLEY. No.

Mr. PASCRELL. Robert MacLean was an air marshal. He was fired for alerting the public that the TSA was going to save money by removing marshals from the very kinds of flights targeted by the 9/11 hijackers. He was fired for that. You are not familiar with that case?

Mr. HAWLEY. No.

Mr. PASCRELL. Mr. Hatfield, are you familiar with that case?

Are you familiar with that case, Ms. Berrick?

Ms. BERRICK. No, I am not.

Mr. PASCRELL. You are not familiar with that case. Could you get familiar with the case and get back to us about what your perception is of this? Because this, to me, is unacceptable. I would hope the chairwoman would also agree this is unacceptable.

Two security training officers in Buffalo, New York were bounced for telling superiors that bags were being put on planes without proper explosive screening. An acting assistant federal security director was ousted after she complained that her boss was illegally flashing an assault rifle at an Oregon airport. You are not familiar with any of those cases?

Mr. HAWLEY. No, sir.

Mr. PASCRELL. Well, I wasn't making these up.

Mr. HAWLEY. No. I appreciate that.

Mr. PASCRELL. Well, where did they come from? I mean, you are not familiar. You are supposed to know these things that are violations and deficiencies within the system itself. You know, I don't agree—and I am sorry the ranking member, my friend, Mr. Lungren is not here, from California—we can't accept a half-a-glass. That is not acceptable when it comes to the safety of human beings. That is not acceptable. We are not talking about other

issues. We are talking about the protection of those folks who choose to use our airlines. I hope someday we will be talking about those who choose to use our mass transit system, which 50 times more people use that every day as well.

I thank you, Madam Chairlady, for your indulgence, and I thank you, Secretary Hawley.

Ms. JACKSON LEE. We have been somewhat lenient with our members. We know that it is difficult to hold these hearings, and there are a lot of concerns that members have. I thank Mr. Markey for his indulgence, and now I am pleased to yield to the distinguished gentleman from Massachusetts 5 minutes for his questioning.

Mr. MARKEY. Thank you, Madam Chair.

Mr. Hawley states in his testimony that, "TSA will build upon established programs to comply with the cargo screening requirements of the law implementing the recommendations of the 9/11 Commission." This is very troubling because TSA's established program, such as Known Shipper, have been widely criticized for failing to adequately protect the American people from another 9/11-style attack.

The purpose of the air cargo provision in the 9/11 Commission Act is to fundamentally change the status quo and overhaul TSA's established programs. The status quo is unacceptable. I have a pile of reports here that point out the problems with TSA's established cargo security programs. GAO reported in October of 2005 that TSA's air cargo policies have significant problems.

Today, GAO's testimony identifies some of the same cargo security gaps that it uncovered 2 years ago, such as TSA's failure to complete assessments of air cargo vulnerabilities or critical assets, which GAO believes undermines TSA's ability to focus its resources on the most critical security needs.

My question you first, Ms. Berrick, is has TSA completed assessments of air cargo vulnerabilities and critical assets such as cargo facilities and airports?

Ms. BERRICK. The report you are referring to was our review of domestic air cargo security. We have since done an additional report that we issued in April of this year on in-bound cargo coming into the United States. So we have looked at both sides of this, and CBP also plays a role on in-bound cargo.

What we found most recently was TSA is continuing to do threat assessments. They are doing vulnerability assessments of air cargo facilities. They haven't yet completed these as of the date that we did our work in April of this year. So we made a recommendation that TSA move forward and work to complete those assessments.

Mr. MARKEY. So they have not completed them. Is that what you are saying, as far as you know at this point as you sit here, Ms. Berrick?

Ms. BERRICK. As far as I know, up to the date that we did our work and issued our report in April, yes.

Mr. MARKEY. Okay.

Mr. Hawley?

Mr. HAWLEY. Well, I think the bottom line is I think we have closed the gap that may be perceived between what you think on air cargo and what we do, in that we have moved to close these

vulnerabilities. On the Known Shipper program, I would just like to specifically hit that because I do know that in the law it specifically calls out and says that you cannot count Known Shipper as part of what is in the bill. We accept that. We understand that.

The reason I had in there the part about building on the existing was more about the K9 Program and the inspectors, and that we don't feel like we should pull Known Shipper out, but we are in agreement with, I believe, you, and certainly what is reflected in the law here, is that in the system of screening that is required under the law, that under the definition it makes that clear.

So I just want you to know that we are under no confusion that we cannot accomplish what is in the law by relying simply on the existing Known Shipper.

Mr. MARKEY. I understand that. But in your testimony today, Mr. Hawley, you say TSA will build upon our established programs, air cargo security regulations, security directives—the Known Shipper management system, and so, again, by using that terminology and giving that kind of direction to your own employees.

Mr. HAWLEY. We are just saying we are not going to pull it out. It doesn't make sense to pull out that level of security. It is not enough by itself, but it does add some value and therefore should be retained.

Mr. MARKEY. All right. Let me move on. The GAO reported in April of this year that air carriers in some foreign countries inspect air cargo for potential weapons of mass destruction prior to loading the cargo on U.S.-bound flights. But TSA and Customs and Border Protection does not require such screening for WMDs for flights heading to our country.

Mr. Hawley, is it still the case that TSA does not require foreign airlines to screen their cargo bound for our country for nuclear bombs and other weapons of mass destruction?

Mr. HAWLEY. They have screening requirements similar to what we have in the U.S. I don't believes our specifically call out weapons of mass destruction. You are talking about radiation portal monitors, probably. But in the course of the inspection for the regular TSA assignments, anything that would qualify as a WMD would certainly show up.

Mr. MARKEY. Ms. Berrick, do you believe that TSA should require that such screening for nuclear bombs be done?

Ms. BERRICK. We didn't recommend that TSA require that. What we recommended was that TSA consider some of the practices that foreign countries were using. One of those was the use of radiation detection equipment to screen cargo. Another practice was more stringent verification of known shippers. Some countries have a very rigorous process for verifying known shippers before they recognize them as "known." Some countries are using technology more than in the United States to screen air cargo.

So because of these practices, we recommended to TSA that they systematically look at what other countries are doing to see whether or not they could apply some of those practices in the U.S.

Mr. MARKEY. Well, let me just say this. I am very concerned on an ongoing basis, knowing that al-Qa'ida has placed nuclear weapons at the top of their terrorist target list, along with aircraft. I

just want to make this point, Mr. Hawley, that when Congress passed the language implementing the recommendations of the 9/11 Commission, it did so with an intention in the cargo screening area to fundamentally and dramatically change the way in which business was being done.

Congress did not intend for these regulations to have tinkering around the edges. It wanted a fundamental change that put in place the kind of air-tight security that Americans expect when they are boarding planes. My concern is in reading comments in the newspapers and even in looking at some of the language in your testimony, that there has not yet been a full appreciation for the extent to which I, and I think I can speak for the chair of this subcommittee and other members, are going to be paying very close attention to the kinds of programs that you put in place.

Mr. HAWLEY. Thank you. I would just like to say to you personally, so there is no doubt, we do understand and worked with the committee, and I truly appreciate the opportunity to work with the committee during drafting. We fully expect and intend to meet the requirements under the law passed by the 9/11 Commission. We do understand the changes that are included here. We are also grateful for the 170 K9 teams added in the supplemental. We are continuing to add security for air cargo. Let there be no doubt, we intend to fully meet these deadlines.

Mr. MARKEY. Well, again, as the author of the language on the air cargo issue and on the screening for nuclear weapons on ships coming into the United States, I can tell you that I, for one, am going to watch very closely to make sure that you have put in place the kinds of protections which this law has passed to ensure would be done at the Department of Homeland Security. I look forward to working with you in the months ahead.

I want to thank you all. I want to thank Ms. Berrick and GAO for the excellent work they have done for the committee.

I yield back the balance of my time.

Ms. JACKSON LEE. I am going to offer a second round, but let me thank Mr. Markey for the line of questioning. I appreciate the witnesses in the manner in which they have received them.

I am going to follow up on his line of questioning, because I want him to know that this chairwoman joins him in working to monitor the work that he has led on. Here is the question, and don't think, Assistant Secretary Hawley, that I am not mindful of the deadlines that have been put in place, in fact, the compromises that have been put in place on air cargo inspection.

But let me ask you today, do we inspect 100 percent of air cargo today, Tuesday, October 16, 2007? Does America do 100 percent today as we speak?

Mr. HAWLEY. We are very close to it, in that we have the airlines requirement that has been out there for a long time. It is a classified number that you know what it is. So there is that as the basic starting point.

Ms. JACKSON LEE. But I think, and I will let you answer, do we do 100 percent today?

Mr. HAWLEY. We are pretty close in that—

Ms. JACKSON LEE. But not 100 percent?

Mr. HAWLEY. I don't want to say here today we are meeting 100 percent. We have 3 years to meet the 100 percent under the new law.

Ms. JACKSON LEE. I understand that.

Mr. HAWLEY. But the reason I am optimistic on that is today we screen 100 percent of freight at the small airports to the same standard as checked baggage, so that is 250 airports right off the top. We take what the airlines screen, and then we have the equivalent of 100 K9 teams dedicated to cargo that go specifically at the freight that is not cleared by airlines, and that is at the bigger airports. Then we have additional security measures in place for items that used to be so-called "exempt," but used not to have specific security measures to them that now have those added on.

So from the security point of view, we have very definitely closed down on vulnerabilities that may have existed a year or more ago, and that does not take away from the fact that we still have more to do and look forward to doing that.

Ms. JACKSON LEE. Let me ask unanimous consent that the hearing be allowed to continue past the time of the losing of a quorum. I ask unanimous consent. Do I hear any objection? I do know that the ranking member had intended to return and I am trying to be respectful to see if that opportunity occurs. I thank the committee.

Let me just state for the record that there is not 100 percent screening, and I do recognize what the 9/11 bill, H.R. 1, allowed you. The reason for making that point is the basis of this hearing. We are not where we need to be as the traveling public continues to travel. So I am obviously trying to create a sense of urgency that as we speak today, we have the traveling public flying on commercial airlines and there is not 100 percent screening, which gives us the added sense of urgency, one, to expedite even sooner than the 3-year timeframe, which really was a compromise; and two, to recognize the need for this hearing and the importance of collaboration between the agencies.

Let me continue my line of questioning to ask again, assistant secretary, whether or not one of the issues that Mr. Markey is made is a technology question, particularly as it relates to nuclear. We have said over and over again to many of his inquiries that it is really questionable whether we have the technology or questionable whether or not we are determining whether or not, and this has to do of course with the ship, but radioactive material, for example, that could be shipped or could be transported by airlines. It could be in a suitcase.

My question to you, because this is so significant, are you engaged with stakeholders in the private sector to solicit that expertise to be of help in developing technology that can speed along the 100 percent air cargo inspection that we are looking to? Since we have engaged previously with the private sector, where are we in making sure that we are astutely looking for new technologies to assist in moving quickly on 100 percent air cargo inspection?

Mr. HAWLEY. The process for that is the Science and Technology Group at DHS, which has responsibility for new technology. So they are very heavily engaged with that, as is the DNDO, the nuclear office at DHS. So they have responsibility for the new technology. But I do have to add that the screening that we do for the

regular cargo, as well as for checked baggage, is also good security for anything, even without the radiation monitor, that would represent a threat of any kind.

So I think we are all striving for more and better technology, but the existing process is a good security system that would pick up threats of any kind.

Ms. JACKSON LEE. Well, could I ask you on the record to be diligent. We have just asked you and Mr. Hatfield and the FAA administrator to coordinate. May I ask you to engage your colleague, because it has come to our attention that that is a very slow process, and that technologies from the private sector are moving more slowly than they should. That is why I wanted to have on the record that we in fact today do not have 100 percent screening of cargo.

Let me quickly ask these questions of Mr. Hatfield. Would you go over for us—again I use the term "quickly," and I apologize because there are a series of questions that I have—the general guidelines that the FAA adheres to in responding to a terrorist-related incident? And let me appreciate your service on 9/11. I could not imagine not being in your shoes what that experience was about, or what it was like, rather.

I will say that we need to do better in hindsight, and you just offered an additional thought for this committee, is the Department of Defense, because we believe in jurisdiction, but we also believe in security. And you have said you added them at a later time, and they were certainly a strong component of that day. We thank you for your service. I would like to know what guidelines you engage in now if a terrorist incident, you needed to respond to that.

Let me ask Assistant Secretary Hawley what and how often do you engage with the FAA in tabletop exercises addressing in-flight security? One of the issues, of course, is to make sure that we are addressing security issues, as opposed to unfortunate missteps by passengers who may travel in-flight. I wanted to know what kind of training do we have addressing in-flight security.

Ms. Berrick, you have been kind with respect to how far TSA has gone. You said 70 percent, but I am still uncomfortable with your answer in terms of whether or not the situational exchanges are enough. I will ask you the question. Are we at 100 percent perfection? Because as you well know, you have 70 percent, if you will, success, but 30 percent vulnerability. That is a terrorist act.

So I would really like you to be pointed in your answer. I think you have on the record that they have made strides, but are we at a point where we are at a sufficient level of communication? Is it quick enough, frankly? Because terrorist acts don't make appointments, and they don't move slowly.

So if you would, Mr. Hatfield, answer the questions that I have just raised with you, and Mr. Hawley.

Mr. HATFIELD. Certainly. Your question is what have we done to basically document the procedures and the guidelines that we use during a crisis. Our primary tool is the domestic events—

Ms. JACKSON LEE. Within limits, can you address what are the guidelines? How do you move forward in responding to a terrorist-related incident, obviously, without venturing on classified information?

Mr. HATFIELD. I know on the surface that appears to be a simple question, but it is not. It is very complex. Any situation that we encounter starts out, the vast majority, as a nonterrorist threat. It starts out with an anomaly that is being observed usually by an air traffic controller, or a piece of information that TSA has passed to us about a particular airplane.

The protocols for working aircraft from hijacked aircraft to aircraft with lost radios, all of those used to be in a lot of different locations. They have all been consolidated and put into a training package which is obviously a very sensitive thing to be discussing openly. Those procedures are memorialized, but a typical scenario develops from one where we might have a no-fly individual onboard an aircraft. Immediately, the DEN is engaged with the FAA–DOD–TSA.

At the same time, concurrent with that, Kip Hawley and I are on a telephone personally with one another and our staffs. He is telling me what he knows about the airplane, and I am telling him what I know about the airplane. And we make a decision. Are we going to divert the aircraft? Are we going to allow it to continue to its destination? Are we going to turn the airplane around? Are we going to send it to another country?

It is a number of variables that are very difficult to package into a set of guidelines. Is the person asleep? Is the target individual on the aircraft awake, agitated, walking around? All of those variables are weighed, and a decision is made collectively between TSA, FAA, and if necessary, DOD, as to the appropriate course of action. Those procedures from the domestic events network are documented. Training has been given to the air traffic controllers, in follow up to an earlier question or observation that you had made. Computer-based training, CBI, was administered in February of this year. Round two of that training will be administered in November of this year.

So I hope in some way I am addressing your question.

Ms. JACKSON LEE. Let me thank you. I am going to hold. We are in our second round.

Ms. Clarke, would you care for a second round?

Mr. Pascrell?

Excuse me, I will be in a third round, so let me ask Mr. Hawley and Ms. Berrick to hold those questions that I gave.

Mr. Hatfield, you have given me a fair answer. Thank you.

Mr. Pascrell?

Mr. PASCRELL. I would like to ask a question about the airport perimeter security, if I may. GAO identified 24 performance expectations at TSA, of which 17 were generally achieved and seven were rated as generally not achieved. The performance expectations that were generally not achieved included the failure to establish standards and procedures for effective airport perimeter security.

In 2006, it was reported at Newark Liberty Airport, an inebriated passenger briefly got onto the tarmac by improperly walking down a jetway staircase after arriving from Puerto Rico. In addition, two homeless people wanted for parole violations in Georgia were able to enter the airport secure area by lifting the bottom of a chain link fence and getting through that way.

These are just two reports at one airport which simply highlight the vulnerability of our nation's airports to intrusion through breaching the perimeter. The Port Authority of New York and New Jersey has tried to address this vulnerability through a $138 million system that would surround Newark Liberty International, JFK, LaGuardia and Teterborough Airports with a mix of radar, infrared sensors, video motion detectors, closed-circuit TV monitors, and fiber optics as well.

This system would be designed to detect human motion and help prevent potential intruders from breaching the perimeter of the airport. This system is modeled after others already in use in Baghdad and sections of the Israeli border. However, apart from the efforts of the port authority, as well as a similar system at Logan Airport in Boston, I am not aware of any other perimeter defense system at any other airport in the United States.

So my question to you, Mr. Secretary, is if any other airports have a similar perimeter security system in place? More importantly, where is TSA's plan to address this clear vulnerability to the integrity of our nation's airports?

Mr. HAWLEY. The issue of perimeter security is addressed individually at each airport with their airport security plan, where it does specifically address that. I think what you are getting at is the issue of the economic model that we are operating under, which is the airports themselves are responsible for the costs, and it is a shared responsibility on security, and that falls in their bailiwick. The federal government picks up the cost of the security operations in terms of what you normally see at the checkpoints and some other things.

Mr. PASCRELL. Well, what about the model? Shouldn't that come from the federal government as to what are the minimum requirements needed around each of these airports?

Mr. HAWLEY. Yes.

Mr. PASCRELL. This is a very serious situation.

Mr. HAWLEY. Yes, and that is the case. When you get to the more advanced type of equipment, as you are describing, then cost does become an issue. I should just say the port authority is a fabulous partner in this, and we are working with them very closely on all the security matters. The major thing is we need to have layers. It is not just the fence. It has to be layers all the way through, and you have to have overlapping systems where you are not just building a Maginot line, so to speak.

So I would rather have a number of different layers conducted by different people with different systems, than to just place all my bets on one.

Mr. PASCRELL. Well, how many airports have these?

Mr. HAWLEY. This kind of a system?

Mr. PASCRELL. Yes, of the major airports.

Mr. HAWLEY. Well, I think there are probably components of them. I am not aware of actually what the one you are describing is in all of its attributes, but I think the $138 million you mentioned sounds to me like I would be very surprised if any airport has on its own put out that money for that kind of a system.

Mr. PASCRELL. So in other words, if the port authority put up this money, if other airports don't have that money, then they just will not get the perimeter——

Mr. HAWLEY. Well, they may be not be able to get that particular one in that particular configuration, but what we would require, and you just said it a minute ago, was that we require the minimum configuration and we have to deliver the security that says, just as you describe, that does not let terrorist acts occur in this airport.

Mr. PASCRELL. Is that public information?

Mr. HAWLEY. The airport security plan is not public information, but is something clearly we would be most welcome to brief with you anytime.

Mr. PASCRELL. Okay.

Thank you, Madam Chairlady.

Ms. JACKSON LEE. The gentleman's time has expired. Thank you, the few times that we would say that. Thank you for your questions.

Mr. Perlmutter of Colorado. I yield the gentleman 5 minutes.

Mr. PERLMUTTER. Thank you. I appreciate your letting me ask questions here at the end.

I will start with something that Mr. Hatfield mentioned in his opening remarks, and that is the World Series. We have the World Series coming to Denver, Colorado. We are very proud of that fact. Having the World Series coming to Denver, Colorado means there is going to be a lot of pressure on the Denver International Airport, the DIA.

So Mr. Secretary, I have a couple of questions for you to start with. The first is, staffing levels. With that kind of a crowd coming, and the fact that there will be so much. It is not a national security event or national security special event, or whatever those are called, but it is close. What steps is the TSA going to take to move people through the airport? Because as much as you and I have talked about it, there has been some improvement, but then we see our wait times growing because we are not adding people to the TSA staff. Can you please answer that?

Mr. HAWLEY. The short answer is whatever it takes to make the World Series a success. We do this for the Super Bowl, World Series. We bring in extra people. We understand the major importance. It is an international event. That is not an issue. I think the issue you mentioned after that, which is the sustainability and to get the staffing right at Denver, as you know that is something that we are triggered on. You may know that we have just recently added in the 2008 allocations some significant new resources for Denver.

So the key thing, as you know, is opening early. And so yes, we are dialed-in on that. But as far as the World Series is concerned, we are going to support Denver totally, except that I am a Red Sox fan.

[Laughter.]

Mr. PERLMUTTER. I was going to quote you. I was going to put that you were going to support us. I appreciate that.

Let me move now to something, though, that causes some delays from time to time, and that is the no-fly list and the Terrorist

Screening Center and its lists, whether it is the terrorist watch list, no-fly list, selectee list. What steps do you know—and this applies to Ms. Berrick, too, if you could talk about this—what kinds of scrubbing of the no-fly list is occurring so that we don't have misidentifications or delays for folks who clearly don't fit the profile?

Let's take Sam Smith, you know, who had done something bad in Northern Ireland 15 years ago, and a Sam Smith who is 10 years old in Denver, Colorado is being stopped and screened twice. How are we dealing with scrubbing these lists or making them better and less inconvenient for folks?

Mr. HAWLEY. I can answer the first part of that, which is we went through every name on the no-fly list with the Terrorist Screening Center and cut the list in half. And that was part of the effort to prepare for Secure Flight. So that is an ongoing effort. We are now addressing the selectee list, which will also get at a significant number of people.

Mr. PERLMUTTER. Is this something you are doing on an ongoing basis, always going back and looking at these lists to make sure that they are applicable?

Mr. HAWLEY. Yes. And the other piece is that whenever a name comes up, because obviously when one pops up, we are always look at it for, is this the right level of attention? Is it a no-fly? Is it a selectee? I think we had one yesterday that was a no-fly, but in the post-mortem we all decided let's move it back to a selectee. So that is something we do real-time. We want to get as many people who shouldn't be on that list off that list.

Mr. PERLMUTTER. Ms. Berrick?

Ms. BERRICK. Yes. The Department of Justice IG, and in fact GAO also just recently issued reports on this topic. We would be happy to come and give you a lot of details on those. But generally we reported similar information that TSC, working with the agencies, including TSA, have done scrubs of the list, including the no-fly list.

We have identified some issues with the scrubbing process and still identified some hurdles that TSA had to overcome, but generally the list had been reduced and they had been scrubbed. It is a continual process that TSC is going through to do that.

Mr. PERLMUTTER. Okay. Here is the bottom line for the traveling public, and I think for members of Congress. We spend billions of dollars for equipment and staffing and zillions of dollars in wait-times of passengers. Is all of this worthwhile? Or is it window dressing?

Mr. HAWLEY. It is critical. I think the whole issue of the threat level we are facing and the plots that we know are ongoing in the world, and the interest in attacking the United States is absolutely critical. I think the experience really since June abroad is instructive to us, and last year, the liquid plot. These are people bringing liquids on planes to blow them up by the dozen.

So it is absolutely critical. I think that Ms. Jackson Lee at the beginning of the hearing mentioned a little bit of the fatigue factor of how do you keep up the vigilance this far out of 9/11 when the public doesn't see it every day. We sure see it and our officers see it. I would just draw attention to the toy cars thing that we put

out a couple of weeks ago, which is this is the first time we have done it.

In a low-key way, we briefed our officers on the intelligence related to that. And we said, "You know what? Let's just say it to the public that we have some information on this, that we are taking into account in our security measures." We are not prohibiting anything. We are not getting hysterical over it, but we just want you to know we are paying attention, and if you notice something different with the way we screen these things, it is for a good reason.

So I can tell you absolutely for certain it is necessary and clearly, as has been pointed out, we can continue to do a better job, but we feel it every minute.

Mr. PERLMUTTER. Mr. Hatfield or Ms. Berrick, do you have any comments?

Ms. BERRICK. I can just add that during the course of our work, we always look at the intelligence information for different aspects of aviation security, and how TSA uses intelligence to drive its security decisions. I would agree that there is incredible intelligence information that they are using to try to identify where they are vulnerable and what actions they should take to address that. So I think that is a very important role.

And then secondly, the security measures also act as a deterrent to persons intending to do harm. They see the measures that are in place. They see that some of these measures are changing. They see that there are layered security measures. All of those are obstacles that they would have to overcome to act. So I think that serves an important function, too.

Mr. PERLMUTTER. Mr. Hatfield, any comments? Or do you go along with those two?

Mr. HATFIELD. No, sir. I would go along with those two comments. Thank you.

Mr. PERLMUTTER. Thank you, Madam Chair.

Ms. JACKSON LEE. I thank both Mr. Perlmutter and Mr. Pascrell.

I yield myself 5 minutes for a third round, and cognizant of the time.

This has been a burden on the subcommittee in terms of trying to get to a sense of wholeness on the aviation. I am going to quickly ask you to quickly answer the questions that remained. Mr. Hawley, that was on in-flight security, FAA and tabletop exercises. If you could just do that very, very quickly, and Ms. Berrick. And then I am going to go into some other very what I consider questions that remain on the table.

If you would, Mr. Hawley?

Mr. HAWLEY. We do two formally a year at the administrator level—the FAA administrator and myself, as well as our key staff, twice a year formally. I would venture to say we probably do about one a month of the type that Frank mentioned, something that comes up during the day or night. You asked the question, how quickly do we respond, and I would say it is immediate. We always have a duty officer, either Doug sitting back there in the front row, or Frank is on duty 24/7. We frequently talk in the middle of the night if required.

Ms. JACKSON LEE. Ms. Berrick, remember I asked you about how perfect is the situational exchange, because that is a question of life and death.

Ms. BERRICK. Right. You referred to the 70 percent. I just wanted to clarify. That is our overall assessment, the degree to which TSA has met the requirements that were laid out by Congress and the administration, and that is covering all aspects of aviation security. Again, the key areas that weren't being addressed that we reported on were technologies at checkpoints and to screen air cargo. There was also perimeter security and access controls. And there was also a system to pre-screen passengers on domestic flights.

With respect to communication and coordination between TSA and other agencies, again we reported that from what we looked at, it was generally working well. We looked at over a 3-year period. There were some breakdowns in communication, but generally the process was working well. That has been put in place since 9/11. But we did identify the importance of each of the agency's involved documenting their policies and procedures. I know the FAA has documented the procedures. Some agencies don't.

When we are talking about 15 agencies—DOD was mentioned—but there are a lot of other agencies involved in this coordination effort, too. Even though the people in place may know how to respond in situations, they have built relationships. If they have to leave those positions, it is important that these procedures be documented and memorialized.

With respect to the exercises, we did review that and saw that the agencies were holding exercises to look at different scenarios and how they would respond. The one area for improvement we saw there was the need to follow up on action items from the exercises. So for example, issues may be raised during the exercises, but there always wasn't that follow up afterward to make sure that the loop was closed so any issues raised were addressed.

Ms. JACKSON LEE. If you had to assess how quickly today they coordinate, versus before 9/11, do you have that ability? How quickly does it occur? There is an incident in the sky. We don't know what it is. How quickly can these different entities gather and begin to respond?

Ms. BERRICK. I would say it is almost immediately because the domestic events network, the DEN, is up 24/7. Everybody is tied into it, all the agencies that have roles and responsibilities related to coordinating these incidents. So information is broadcast over the DEN for all to hear. People are brought into have that discussion. They can share information.

In terms of how it is different now versus before 9/11, before 9/11 the DEN didn't exist. It was created on 9/11.

Ms. JACKSON LEE. So an incident occurs, and you are saying almost immediately the coordination occurs or one agency knows about it?

Ms. BERRICK. Almost immediately the communication occurs, because all relevant agencies are tied into the DEN, because it is a 24-hour network. So they can get information immediately as it is relayed to them.

Ms. JACKSON LEE. Let me thank you. I assume the agencies are monitoring that, and your one addition is that they need to document in more detail on how that is occurring.

Ms. BERRICK. Exactly—how they would respond under different scenarios.

Ms. JACKSON LEE. Thank you.

I am going to do a rapid series of questions. I would appreciate if the witnesses would take notes, so that then I will yield to you to answer the question.

Just for you, Mr. Hawley, I have an issue that is similar to Mr. Pascrell. Would you please investigate, as I have asked you previously, Mr. Roy Ray, a TSA screener—I would like to put that on the record—who has had some similar issues that Mr. Pascrell has mentioned. His name is Mr. Roy Ray. I would like to have that investigated, if I could.

Let me just say that this committee hearing and the one that will come will include, or is including the question of general aviation. I want to cite in particular an investigative report done by Channel 11 News in Houston that found the airport security at small airports to be very lax. In response, I wrote a letter to Inspector General Skinner to investigate these breaches in security. Further, when I questioned Secretary Chertoff he admitted in a hearing that we needed, you needed, to turn up the temperature on general aviation.

Today, unfortunately, it has been 8 months and no investigation has occurred. General aviation airports across America remain vulnerable as it relates to perimeter intrusion and they are still flying in and out, and some of them large planes that have the capacity for much damage.

Moreover, the inspector general's office has claimed that they do not have the funds to conduct an investigation this year. Why is that? And I will be asking a series of questions on that question. Security at small airports continues to be unacceptably lax. We would like to know what steps TSA is taking.

Now, we understand that there is a jurisdictional question in law, and a question where TSA is not present at general aviation airports. I would hope that we are laying the ground work—and Ms. Berrick, this question is for you—on possibly having expanded legislation to address the question of general aviation airports.

Let me just speak directly to the perimeter question. One of the indicia or reports that you gave that said generally not achieved had to do with the perimeters, where you asked TSA to establish standards and procedures to effective airport perimeter security, That is obviously the larger airports; establish standards and procedures to effectively control access to airport secured areas, not achieved; establish procedures for implementing biometric identifier systems for airport secured areas access control.

This could be similarly connected to general aviation if you were looking at it, and I don't know if you were, but I would appreciate a response. It says that in perimeter issues, the TSA has not achieved what it should achieve. That is one question.

The second question goes—Mr. Hatfield, if you would just listen—I maintain that you all, the air traffic controllers and the FAA as it relates to air traffic controllers—do a yeoman's task, a very

important task. However, I am disturbed by numbers that I would like to share with you. In 1985, there were 34,000 air traffic controllers. In between that, there was the Reagan issue in 1987. In 1990 there were 36,000. I am now looking at a document that says that now today, 2005 and 2006, we have approximately 14,000. In fiscal year 2006, we have 16,000 air traffic controllers. In fiscal year 2004, we had 17,000, which was already half of the 34,000.

Now, I imagine that you will give me an answer that might suggest that we have great technology and so we don't need it. I think it is a travesty. I think the lack of air traffic controllers experienced and trained from my perspective, which is one of the reasons why you are here, Mr. Hatfield, has a definitive impact on the security of this nation and the traveling public. I might suggest that you have an answer to that, and these are my final questions.

Let me thank you, Mr. Hawley, for the work you have done and tried to do with respect to racial profiling, in particular dealing with headdress. I want to make sure that every traveling person is given the dignity of who they are and not being a terrorist, or not being felt that they are terrorists by their, if you will, prayers or their headdress. So I would like you to comment on that and how you have been able to address that question.

I would add to this in a very tragic way, a reference—and let me make it distinctive so that we don't have a misunderstanding of media or anyone else—I would like to at the same time have a full report on the situation dealing with Ms. Gotbaum. I raise that because there was language that said "I am not a terrorist." There was also some reporting that TSA employees did either encounter or ask questions. I am not sure what occurred, but we want terrorists to be found and arrested. We want the traveling public to be addressed in whatever human condition they need to be addressed in.

So I would like to ask on the record for a full investigation as it relates to any TSA involvement in that second incident that I mentioned, and you can respond to the issue dealing with the headdress that I believe is an announcement that was made today.

Let me start with Mr. Hatfield on this question of half of the size of, as I understand it, of air traffic controllers some 10 or so years ago, compared to today of 16,000—a number that has been going down. Mr. Hatfield? As it impacts security?

Mr. HATFIELD. Well, you asked this question, chairwoman, earlier. I have to tell you it is a very tough question. I have never looked at in the terms that you have asked. The way I interpret it, how many controllers do you need to make sure you have enough controllers so the sky is secure. Quite frankly, that is never something I have ever thought about before.

I think the best way I could answer that is, my core mission is safe. Certainly, if I have enough controllers to keep the skies safe, then certainly I have enough controllers to keep the sky secure.

Ms. JACKSON LEE. And you think you have enough, compared to 34,000 10 years ago and now 16,000? Haven't you lost a large number of experienced controllers?

Mr. HATFIELD. Certainly, I can't contest the fact that there has been a loss of experienced controllers in the sense that people normally retire. But what I can say is I know for a fact that for the

last 3 years, the FAA has had a target goal of hiring. They have hit it for the last 3 years. I know in fiscal year 2007, 1,800 controllers were hired. I also know that system-wide right now, we are running with overtime of less than 1 percent, which is a pretty amazing statistic for a company that big.

So I will contend that the system is safe, and if the system is safe, then certainly the system is secure.

Ms. JACKSON LEE. Let me ask that you give more thought to that, and possibly respond in writing. I thank you for your answer on that.

Mr. Hawley?

Mr. HAWLEY. Yes. On Mr. Ray, I have had the chance to look into that. I believe I am writing you a letter, but I have looked into that and can respond to you specifically on that.

Ms. JACKSON LEE. Thank you.

Mr. HAWLEY. On the general aviation perimeter—and I will put that in with general aviation security generally—we are looking at on a risk basis the GA community, and separating by the threat presented by aircraft. The critical issue is the identity of the pilot. That, to me, is the most important thing. There are a lot of other physical security and other matters that have to be in there, but understanding so that the FAA knows who is the actual pilot in that aircraft positively, other than just the honor system, I think is the critical point. We are working with our international colleagues to get that.

On the headwear——

Ms. JACKSON LEE. Mr. Hawley, you answered part of the question. The Channel 11 investigation in one city, it happened to be Houston, showed the rapid and continuous piercing of general aviation perimeter, meaning that it is a vulnerable target because it has none of the security measures of regular airports, even though as you well know, I just noted that you generally had not achieved perimeter security on airports that are under your supervision. Would you not think that legislation might be warranted to include general aviation airports in some sort of security control, in as much as larger airlines, large airplanes land at general aviation airports?

Mr. HAWLEY. We will look at that. I think another key is the physical security of the aircraft and the ability to turn on the aircraft, basically, if you don't own it, and then there is another way to get at some of these problems. Certainly, physical security is an important part of which perimeter control plays a role as well. That I will have to look at, but I will look at that.

Ms. JACKSON LEE. You will provide a report back to this committee?

Mr. HAWLEY. Yes, ma'am.

Ms. JACKSON LEE. Thank you.

Mr. HAWLEY. On the headwear, we had some issues with members of the Sikh community who were concerned that the effect of TSA screening of headwear would single them out for extra treatment. They have entered into a conversation with us that I think was very healthy on a number of fronts. It helped us set up, and now we have a Diversity Council that we work through with these issues. We do understand that the Sikh community is on our side.

We are on the same side, and we have some up with a headwear screening method that meets the security and also the dignity and common sense, not only for people with religious headwear, but medical or other needs as well. So that we have put out today.

And then the last one, the tragedy in Phoenix, we will investigate it. The initial reaction is that there was one transportation security officer in Phoenix who had contact, but it was only to render assistance when it looked as if the individual was having a problem. I believe we have the video for that and we will do an investigation, as you suggest.

Ms. JACKSON LEE. I appreciate it.

Mr. Berrick, if you would conclude by focusing on the question dealing with general aviation, on perimeter security, and whether or not you have a study that deals specifically with general aviation perimeter vulnerabilities.

Ms. BERRICK. Okay, sure. We have looked at both areas. The general aviation work we did was 3 years ago when we looked at it. At that time, TSA was in the early stages of looking at GA security. They had developed a voluntary self-assessment vulnerability tool that GA airports could apply, but that was in the early stages. Some of the states had more stringent requirements for GA airports. Some of the states were pretty active. Others were less active.

There are security requirements for foreign students that take flight training at U.S. flight training schools. We looked at that process and the checks that are conducted of these students. We identified some problems there and made some recommendations. The specifics are classified and we could certainly brief you on that.

And then, of course, there are some security requirements for larger GA aircraft. We are not doing any follow-up work right now on general aviation, although some committees have expressed an interest in GAO maybe doing some additional work.

In perimeter security and access controls, we did a review again in 2004. Recently, as a part of our report card on DHS, we got updated information from the department on its efforts to secure perimeters and access controls. The area where we identified DHS was primarily lacking was related to technologies, providing information on technologies to the airports. There are lots of legislative requirements that require TSA and DHS to do that. There is no widespread biometric system at the airports, so it is primarily focused on technology. And there are some other legislative requirements also that weren't met.

We are actually doing follow-up work now on airport perimeter security and access controls for you and for some other committees that we have recently kicked off. We can come and brief you or your staff at any time on what we are finding on that. But that work is underway right now.

Ms. JACKSON LEE. We would welcome that. Ms. Lowey of New York has been a champion of that issue. So we would like you to finish your work.

I want to go back to general aviation as I conclude. Is there a state that is a model for general aviation security? You mentioned that there might be some states.

Ms. BERRICK. There are some states that are stronger. I will have to get back with you on the specific names because I am not remembering them right now. There were a few states that stood out in terms of requirements in locking the aircraft and fencing and some other requirements at some GA airports. So I can follow up with your staff, if you would like, and provide that information.

Ms. JACKSON LEE. In your general assessment, one, I think the committee and I will certainly raise this with the chairman of the full committee, that we would like to have. As I indicated, the inspector general has not responded to the inquiry on the vulnerabilities of general aviation airports. So we have a real problem.

My question is, just in the overview that you did 3 years ago, and you can reflect on it, do we still have some gaping security, if you will, holes in, as you can reflect, on general aviation perimeters and general aviation sites in the United States?

Ms. BERRICK. I would say based on the work we did 3 years ago and some limited updated information, I would say that more work is needed to assess what the vulnerabilities are and what the options are for addressing those vulnerabilities. Again, at the time in terms of doing vulnerability assessments, TSA had developed this tool and was sharing it with the operators, but that was in the very early stages. So I think more assessment and attention is appropriate. I think it would be worthwhile to look to see to what degree it is happening today.

Ms. JACKSON LEE. So general airports or aviation sites could be vulnerable to terrorist acts?

Ms. BERRICK. I think so, as a lot of other sites and locations could be vulnerable as well.

Ms. JACKSON LEE. Let me just, we would appreciate your response back on states that might be a model. Frankly, a number of us believe that legislative intervention is necessary on general aviation airports, and we want to be as detailed as we possibly can be in that consideration.

Let me ask if any of my colleagues have a question. Let me thank them very much for their presence here today. Let me suggest that any members will have 5 days to submit any additional comments for this hearing.

I want to take the chair person's privilege to particularly give these witnesses the award for stick-to-itness and presence. This is something that has been mounting. It is very difficult to hold hearings and to gather people and to get the questions that are necessary for what we are attempting to do in securing America.

So let me thank all of the witnesses for their valuable testimony, and the members for their questions. The members of the subcommittee may have additional questions for the witnesses, and we will ask you to respond expeditiously in writing to those questions. I would also ask, because we simply sometimes leave questions on the table to the witnesses, and sometimes there is a delay. We raised very important questions today that have a lot to do with moving forward. We would appreciate as expeditious a response as possible in the light of what we have posed to you.

Therefore, hearing no further business, a thank you, and the subcommittee now stands adjourned.

[Whereupon, at 5:02 p.m., the subcommittee was adjourned.]

VerDate Nov 24 2008 07:10 Sep 04, 2009 Jkt 000000 PO 00000 Frm 00067 Fmt 6633 Sfmt 6601 H:\DOCS\110-HRGS\110-77\48972.TXT HSEC PsN: DIANE

AVIATION SECURITY: A FRONTLINE PERSPECTIVE ON THE NEED FOR ENHANCED HUMAN RESOURCES AND EQUIPMENT PART II

Thursday, November 1, 2007

U.S. HOUSE OF REPRESENTATIVES,
COMMITTEE ON HOMELAND SECURITY,
SUBCOMMITTEE ON TRANSPORTATION SECURITY AND
INFRASTRUCTURE PROTECTION,
Washington, DC.

The subcommittee met, pursuant to call, at 3 p.m., in Room 311, Cannon House Office Building, Hon. Sheila Jackson Lee [chairwoman of the subcommittee] presiding.

Present: Representatives Jackson Lee, Norton, Clarke Lungren and Brown-Waite.

Also present: Representative Pascrell.

Ms. JACKSON LEE. The subcommittee will come to order. As I do that, let me again thank you for your patience, but also your presence here today. I acknowledge the presence of the Ranking Member of the Subcommittee on Transportation Security and Infrastructure Protection, Mr. Lungren of California, and acknowledge the presence of the distinguished—the distinguished gentleman from California, and the distinguished gentlelady from New York, Congresswoman Yvette Clarke of Brooklyn, New York. And I say that because this is an important hearing, and sometimes our schedules are not our own, and it happens to be that way today.

And so the subcommittee is meeting today to receive testimony on the training of transportation security offices, flight attendants and Federal flight deck officers. However, before I begin, I ask for unanimous consent ahead of time that Mr. Pascrell, a member of the full committee, to sit and question the panel during today's hearing. Hearing no objection, so ordered.

I would like to take this opportunity to thank you all for joining us this afternoon. I cannot express the appreciation because of the responsibility that this committee has. And it was designed in particular to delve into areas that heretofore had not been looked at as keenly as we might have wanted to do. And that is not only transportation security and infrastructure protection, but the frontliners that address these particular entities.

As we all know, civil aviation security exists to prevent criminal activity on aircraft and in airports. This activity includes acts such as highjacking, air piracy, damaging or destroying aircraft in near-

by areas with bombs, and assaulting passengers and aviation employees. Today aviation security is high on the list of priorities of air travelers, the Federal Government and the international air community. In the earliest days of aviation, however, aviation security was only a minor concern.

Since September 11th all of us have changed our outlook and perspective, and we have made many improvements in the backdrop of 9/11 in the security of our Nation's transportation infrastructure. It is a work in progress, but there is more work to be done.

However, our job is far from over. Whether it is more improvement to be made or gaps to close in matters of security, we must not become complacent. As our enemies adapt, so must we, and we did. We now have a Federal screening workforce. We screen 100 percent of the checked baggage. We are in the process of moving to 100 percent screening of air cargo. And we are constantly trying to find new technology to help all of these functions; however, it is important to note that there are challenges, and that we should address those challenges. In addition, we armed pilots and barricaded the cabin door.

Some may have agreed or disagreed on some concepts, but the effort was in place; that we must protect the employees and the traveling public. TSA has taken steps to secure the plane and the passenger, but has left the system vulnerable to attacks. In essence, I believe that our focus has only been on protecting aircraft from past attack scenarios, such as suicide hijackings and baggage and luggage bombs carried by airline passengers, and has not given enough attention to other potential vulnerabilities.

Flight attendants, Federal flight deck officers and Federal air marshals are the last line of defense when it comes to security of a plane; however, flight attendants do not receive any meaningful training to protect themselves or other passengers or to thwart a terrorist attack. In the case of the Federal flight deck officer, they do receive training; however, this training does not provide the Federal flight deck officer with the support and mentoring that other Federal officers receive to accomplish their respective missions. These officers should have the same level of training and support that other Federal officers receive so that they will succeed in their mission. This includes post-basic training mentoring and ongoing training.

Finally, there is no comprehensive training or explanation of what the three components of in-flight security flight attendants, pilots and air marshals are trained to do in case of an attack. Clearly these three groups must be trained on how to work together as a team to be effective as possible, because determining how to handle an attempted hijacking should not happen at the moment it occurs, but rather during training events on the ground.

As you can see, coordination is extremely important when securing our planes. We must make sure that these groups are aligned to work very closely in terms of understanding and implementing their roles when responding to an aviation security, a threat.

It has also come to my attention that TSA that designs the scheme, if you will, of how we handle airport screening and where resources are utilized may, in fact, though they are not present at

this hearing, need oversight by this Congress. There is representation that with the movement of TSA screeners, with the assignments being given, opportunities that appeared in Phoenix and other places where the GAO has made studies about intrusion of undetected bombing equipment, that there may be a problem that we have to address.

Additionally, I would like to offer into the record a letter sent to me by a member of the air traffic control, Houston Air Route Traffic Control Center, and an individual who is vice president of the local at Houston ARTCC. I would ask unanimous consent. Hearing no objection, it will be submitted.

Ms. JACKSON LEE. But let me just focus briefly as I conclude my remarks. The absent individual or entity today are the air traffic controllers. We recognize that their vital role deals with the safe travel of airplanes throughout the Nation's skies, but anyone who focused on 9/11 recognizes their frontline responsibility as relates to security as well. And so I am going to state on the record that we expect to have the air traffic controllers present at a hearing prospectively so that we can focus on the needed enhanced security equipment that might make them better qualified and equipped to address any potential threat that might come.

The record should note that I am disappointed, this committee is, of the lack of recognition of their importance in this process, and we hope that that lack of recognition can be quickly amended, and that they will be before this committee, as will the air marshals, who I know are a component of law enforcement present at this hearing. But the comment of this particular individual was expressing concern that I will utilize further in my testimony or my statement as I question the witnesses. But it should be noted that this is in the record, and that the air traffic controllers are not present today, and we expect for them to be present before this committee in the very near future.

Finally, as Members of Congress, and more specifically as members of the Committee on Homeland Security, we have the responsibility to make sure our planes and airports are secure and also our general aviation airports are secure as well, which is an issue that we will be looking at in this committee.

Throughout these hearings I have reiterated that we are at a crossroads where we must take action to find out what is the best way to find a safe, secure and functioning aviation system. In essence, what are the best practices? And if we do not put effective security measures in place, our Nation may very well be the victim tragically of another attack, which in turn will cause a major economic disruption and avoidance of commercial aviation.

We must continually earn the confidence of the flying public in order to ensure that the public continues to enjoy the freedom of mobility that flying provides. We must demonstrate to them that our Nation's airports are secure.

Ms. JACKSON LEE. The Chair is now pleased to recognize the Ranking Member of the subcommittee, the gentleman from California, for an opening statement.

Mr. LUNGREN. Thank you very much, Madam Chairwoman, and thank you for scheduling this hearing.

I would also like to thank the witnesses and the men and women that you represent. We cannot do what we are attempting to do in terms of providing safety in our skies and at our airports without the great work of the people that you represent. We can talk about it, and we can set out rules and regulations, and we can hope that people will act the right way, but it is your folks that actually make the difference.

We have said this time and time again here, as have others, that since 9/11 we have invested billions of dollars to secure our aviation industry. These security investments are necessary because of the continuing terrorist threat to our aviation security. A good example is the improved screening technology we now employ for both checked and carry-on baggage, although we know we have got to keep up with new advances in technology. It is all part of the Homeland Security mission to develop the best technologies, procedures and methods which will deny the terrorist his goal of causing, quote, death and destruction in America.

While technologies, as I say, are important, are necessary to detecting and preventing terrorist attacks, the technology is only as good as our frontline employees who operate it. The better trained these employees are, the better our aviation security will be.

The importance of training was highlighted in a recent news story on covert testing for bomb parts at several U.S. airports. The airport receiving the best grade is just outside my district in San Francisco. The reason for their success is they test their screeners continuously and use the testing as a training tool. The TSA has now adopted this approach in their training programs throughout the country.

Another example of our frontline employees making us more secure is the Federal Flight Deck Officer Program, as referred to by the chairwoman. Arming our qualified and trained pilots has provided another layer of aviation security. Terrorists will now think twice before entering the flight deck of any aircraft. If they attempt to penetrate the locked cabin door, an armed pilot may be waiting to greet them.

There are other things that have been done, but we all know that we can do better, and this hearing is an effort for us to get a status report on how well we are doing in training our frontline employees, what more needs to be done, and also I think to recognize the tremendous role that they play in the overall security for our flying public. And once again, I would like to thank the witnesses, and I would hope that you would let your members know how much Members of Congress appreciate what they are doing and what they continue to do for all of us.

Thank you, Madam Chair.

Ms. JACKSON LEE. I thank the Ranking Member.

Again, let me acknowledge the presence of Mr. Pascrell of New Jersey. We welcome him.

And let me remind other members of the subcommittee that under the committee rules, opening statements may be submitted for the record.

And I join with my colleague Mr. Lungren in again thanking you all for the service that you give.

At this time I would like to welcome our panel of witnesses. Our first witness will be Mr. John Gage, the national president, American Federation of Government Employees, AFL–CIO. In his capacity he stands watch over the rights of some 600,000 Federal and D.C. Government employees. Mr. Gage leads the Nation's largest union for government workers. Mr. Gage has long been involved in the AFGE and the labor movement. He has a commitment of over 20 years of service as president of AFGE, Local 1923, and as national vice president of AFGE's fourth district.

And we certainly had a long-standing relationship, Mr. Gage, and I do thank you for your presence here this afternoon.

Our second witness is Ms. Patricia A. Friend, international president of the Association of Flight Attendants. For the past 12 years Ms. Friend has become a respected leader in the airline industry and throughout the labor movement. Following the September 11th terrorist attacks, Ms. Friend was appointed by Secretary of Transportation, Secretary Norm Mineta, to serve as the DOT Rapid Response Team for Aircraft Security, or serve on that committee, a group of industry experts assembled to recommend aircraft security improvements. Since then she has tirelessly lobbied Congress, the Federal Aviation Administration and the public for their support of more stringent security measures.

The final witness of this panel is Captain Robert Hesselbein, chairman of the Airline Pilots Association National Security Committee. Captain Hesselbein has an extensive background in security. He performed airborne counterdrug intelligence duties in support of the diverse law enforcement agencies and later researched and created the current standard crew member procedures for countering a chemical-biological-radiological, CBR, weapon in flight. Captain Hesselbein has flown at Northwest for 19 years, is a graduate of the prestigious U.S. Air Force Fighter Weapons School.

Without objection, the witnesses' full statements will be inserted into the record, and I now ask each witness to summarize his or her statement for 5 minutes, beginning with Mr. Gage from the AFGE.

Again, welcome to all of you.

STATEMENT OF JOHN GAGE, NATIONAL PRESIDENT, AMERICAN FEDERATION OF GOVERNMENT EMPLOYEES, AFL–CIO

Mr. GAGE. Thank you, Madam Chairwoman and members of the subcommittee.

Among those 600,000 Federal Government workers that we represent are included transportation security officers at airports across the United States. Many times I have testified before Congress of their dedication to doing the best possible job they can to thwart air terrorism. Even as they are wrongfully denied the fundamental collective bargaining rights and labor protections of other Department of Homeland Security workers, the Aviation Transportation Security Act mandated that TSOs receive 40 hours of classroom instruction and 60 hours of on-the-job training before they begin to perform screening duties, and 3 hours of training per week averaged over a fiscal quarter once they begin working. TSOs also

train for proficiency tests that they must pass each year to be recertified. TSA is required by law to provide remedial training to TSOs who do not pass the proficiency tests.

However, TSOs routinely report chronic understaffing at airports, the lack of relevant and low quality of training TSA provides, TSA's failure to fully invest in technology to facilitate the ability of TSOs to evaluate potential threats to aviation travel and TSA's institutional disdain for comments and suggestions from TSO that can help spot and prevent threats to air travel.

First, staffing shortages of TSOs have made it difficult for workers to carry out their duties much less receive statutorily mandated training. TSA has adopted a staffing model that it calls its Staffing Allocation Model or SAM. SAM does not adequately take into account the statutorily mandated training time or other duties TSOs may be assigned, such as administrative work or time to master new standard operating procedures. Even FSDs have consistently reported to GAO and TSA that because of insufficient staffing, TSOs have difficulty in meeting the recurrent training requirement within regular duty hours.

SAM also does not take into account the effect of the incredibly high TSO attrition rate on its staffing assumptions. The first 8 months of 2007 resulted in a TSO attrition rate of 19.6 percent, much higher than the attrition rate of other agencies.

TSA should simply request from Congress funding to fully staff its TSO workforce at every airport. And FSDs should establish personnel schedules at each airport that ensure that every TSO will receive the training required by law while on duty.

The second concern of TSOs regards the quality of training they receive. Much of the training TSOs receive is self-taught, using resources and on-line learning centers. TSOs report that many of these programs are several years old, and often no training instructor is present.

There are striking inconsistencies in the availability and quality in training from airport to airport. One example would be the training offered by bomb appraisal officers, or BAOs. BAOs are deployed at airports and are specifically trained in the detection of explosives. At some airports TSOs report that the BAO occasionally builds a simulated improvised explosive device, an IED, and runs it through the checkpoint to see if TSOs can spot the components. Despite the obvious merits of BAO training to the TSO workforce, at other airports TSOs state that while they are aware that there is a BAO assigned to their airport, the person does not conduct trainings for the TSO workforce.

Over the past few weeks there have been media articles referring to the leak of a classified TSA report that found a high percentage of simulated explosives and bomb parts that were missed by TSOs at three large airports. The reported test results are not in and of themselves indicative of individual TSO or TSO workforce performance. The report does point to a third area of concern to TSOs, that there is an urgent need for TSA to make available updated technology for both passenger and baggage screening. Unlike the covert test of several years ago that involved the detection of fully assembled simulated bombs, these tests often involve very small components that are easily hidden in items that TSA has chosen not to

ban. AFGE TSO members report that even in trainings where TSOs themselves disassembled a simulated explosive and hid its parts in carry-on baggage, they were unable to find the parts by sight alone. Simply put, TSOs cannot be expected to detect what the human eye cannot see.

The technology that would enable TSOs to detect potential weapons not readily apparent to the human eye is available and is currently in use in a number of airports. Repeatedly both GAO and the DHS inspector general have called on TSA to invest in the deployed technology that will assist TSO in performing their screening duties.

Finally, AFGE TSO members report that they have yet to feel that they are a partner working with TSA to ensure aviation safety. According to the 2006 Federal Human Capital Survey, 54 percent of the TSA workforce, overwhelmingly comprised of TSOs, stated that creativity and innovation are not rewarded at TSA. Half of TSA workers report that they do not have a feeling of personal empowerment regarding work processes. Clearly many TSOs feel the agency ignores or discounts their input despite the fact that they serve on the front lines of safety every day at 450 airports across the country.

No worker at DHS should be hesitant to point out a shortcoming that could impact public safety because he or she feels retaliation from management. This is a very real threat to the TSO workforce because TSA refuses to be bound by the Office of Special Counsel's recommendations when TSOs are retaliated against for blowing a whistle on security breaches. AFGE calls or Congress to pass H.R. 3212, a bill introduced by Representative Nita Lowey that would provide TSO collective bargaining rights and workplace protections, and ensure that they are treated the same as other workers at TSA and within DHS.

Madam Chairwoman, the availability and level of training and deployment of technology is incredibly inconsistent among our Nation's airports. But even if the resources necessary to get the job done quickly and effectively and with the valuable input from the TSOs doing the tough job of keeping the public safe, TSA can further accomplish its mission.

That concludes my statement, Madam Chairwoman.

Ms. JACKSON LEE. Thank you very much for your instructive testimony.

[The statement of Mr. Gage follows:]

PREPARED STATEMENT OF JOHN GAGE

NOVEMBER 1, 2007

Madam Chairman and Members of the Subcommittee: My name is John Gage, and I am the National President of the American Federation of Government Employees, AFL–CIO (AFGE), which represents over 600,000 federal government workers, including Transportation Security Officers (TSOs) at airports across the United States. I welcome the opportunity to convey to you the concerns about training that have been a priority issue for our TSO membership since those jobs were federalized over five years ago. Many times I have testified before Congress about the frustrations our TSO members deal with every day as they do everything that they can to keep the flying public safe. I have also testified time and again of their dedication to doing the best possible job they can to thwart air terrorism, even as they are wrongfully denied the fundamental collective bargaining rights and labor protections of other Department of Homeland Security (DHS) workers. The apparent con-

sensus among AFGE's TSO membership is that the Transportation Security Administration (TSA) has made many critical decisions that have created or exacerbated obstacles to the ability of TSOs to carry out their duties, including the availability and quality of training.

The Aviation Transportation Security Act (ATSA) mandated that TSOs receive 40 hours of classroom instruction and 60 hours of on-the-job training before they begin to perform screening duties. After hire, ATSA requires that incumbent TSOs receive 3 hours of training per week averaged over a fiscal quarter. TSOs are also required to pass proficiency tests each year. TSA is required by law to provide remedial training to TSOs who do not pass the proficiency tests. The Government Accountability Office (GAO) described that at least one of the 3 hours is "to be devoted to X-ray image interpretation and the other 2 hours to screening techniques, review of standard operating procedures, or other mandatory administrative training, such as ethics and privacy act training." [1] Our TSO members have reported to AFGE that other than the training they received prior to beginning their jobs screening passengers and baggage, TSA has consistently failed to provide the training they are required to provide under ATSA.

TSOs must deal with the consequences of decisions made by TSA management, from policy decisions made at TSA headquarters, to personnel and scheduling decisions made by the airports' Federal Security Directors (FSD). In summary, TSOs point to chronic understaffing at airports, the lack of relevance and low quality of training TSA provides, TSA's failure to fully invest in technology to facilitate the ability of TSOs to evaluate potential threats to aviation travel, and TSA's institutional disdain for comments and suggestions from TSOs—who stand on the frontlines of air security—that can help spot and prevent threats to air travel.

TSO Shortages

TSA has adopted a staffing model that it calls its Staffing Allocation Model, or SAM. Under the current SAM, TSA's goal is for airports to have a ratio of 80% full-time TSOs and 20% part-time TSOs. SAM does not does not adequately take into account the statutorily-mandated training time TSOs are required to complete or other collateral duties TSOs may be assigned, such as administrative work. Instead, according to the GAO February 2007 report to Congress on TSA's staffing model, SAM assumes staffing levels that "allow most passengers on most days to experience 10 minutes or less wait time," and "that training is relegated to times when there is surplus staffing and should occur during 'less busy times.'" In other words, rather than construct a model that specifically allows times for TSOs to receive the training they are required to have under law, much less time to master new Standard Operating Procedures (SOPs) and technology, this important task is relegated to whatever time is left, even if that time is none at all. FSDs have consistently reported to GAO and TSA that because of insufficient TSO staffing, TSOs have difficulty in meeting the recurrent training requirement within regular duty hours.

SAM also does not take into account the effect of the incredibly high TSO attrition rate on its staffing assumptions. The first eight months of 2007 resulted in a TSO attrition rate of 19.6%, much higher than the current 2.2% attrition rate of the federal workforce. The recent spate of largely cosmetic TSA personnel policy changes have not provided the sort of meaningful change required to maintain the current, dedicated TSO workforce. Since January, 151 TSOs have left Boston Logan, one of the nation's largest and busiest airports. AFGE's TSO members report that at many airports the priority of FSDs is to provide training for new hires and part-time staff at a cost of $10,000 per hire. Training for full-time TSOs is an afterthought. The recently enacted 9–11 Commission Report Act lifted the artificial and arbitrary cap on TSOs. TSA should simply request from Congress funding to fully staff its TSO workforce at every airport. The FSD should establish personnel schedules at each airport that include accommodations for every TSO to receive the training required by law while on duty, and also provide opportunities for TSOs to receive training on new screening technologies.

In addition, TSA can do much to retain and invest in the current full time TSO workforce by dropping its opposition to collective bargaining rights and labor protections for TSOs, by treating them the same as other workers in DHS and the federal workforce. By restoring fundamental fairness to the workplace and addressing those important work-life issues that are pivotal to workers, including training, TSOs will be able to perform with confidence and learn new skills that could lead to promotions and improve safety.

Quality of Training

[1] GAO–05–457, Aviation Security: Screener Training and Performance Measurement Strengthened, but More Work Remains.

Online Training—Much of the training TSOs currently receive is self-taught using on-line resources, or is conducted in the Online Learning Center that provides self-guided training courses. Although initially TSOs reported that there were some airports that lacked access to the high-speed internet capabilities required to run the programs on computers, TSOs now report that at the very least the equipment is available. However, TSOs also report that many of the programs they train on are several years old. Occasionally a Training Instructor (TI) is present, but is relegated to being more of a monitor who can answer questions, and does not provide instructions or elaborate on the online training program. In fact, one TSO told AFGE that he had not participated in a training session led by a TI in over two years.

AFGE's TSO members at several airports have also raised concerns about the qualifications of some TIs. TSOs state that they are aware of individuals who were chosen for the position of TI, but saw no evidence that they were given any sort of training for the job. Multiple TSOs reported that as with other promotions or desirable jobs within TSA at airports, the choices for TI were based on favoritism over merit with friendships, cronyism, and cliques taking priority over training or experience. According to several TSOs, those chosen by TSA management for TI positions had no apparent qualifications for the job, and were chosen over other TSOs who had backgrounds in security, law enforcement, and the military or had previous teaching or instructional experience. Many of AFGE's TSO members came to TSA with those backgrounds, and a belief that their previous experience would be an asset in this country's war against terrorism. Not only is TSA's current policy of favoritism over merit taking its toll on the TSO workforce morale, it is also depriving both TSA and the flying public of the full utilization of all available assets.

"Hands-On" Training—There is no substitute for practical, hands-on experience. This is especially true when it comes to the operation of the X-ray and scanning equipment currently in use at airports. Many TSOs report that they have participated in Threat Image Projection (TIP) where TSOs are required to detect images projected on an X-ray monitor. TSOs consistently report that TIP and other practical training are found mostly at the passenger checkpoint. Despite the fact that TSOs assigned to baggage screening use X-ray and scanning machines just as their colleagues on passenger checkpoint, they are much less likely to receive training on the machines they use everyday. Once again, due to incredibly high turnover rates, at some airports, new hires are the only TSOs who receive hands-on training.

There are striking inconsistencies in the availability and quality in training from airport to airport. One example would be the training offered by Bomb Appraisal Officers (BAO). BAOs are deployed at airports and are specifically trained in the detection of explosives. At several airports TSOs report that the BAO regularly visits both checkpoint and baggage screening and that the BAO occasionally builds a simulated Improvised Explosive Device (IED) and runs it through the checkpoint to see if TSOs can spot the components. At another airport TSOs state that at least twice in the last five years the BAO has conducted a training where TSOs built their own simulated IED and tested each other by running it through the X-ray machine. This type of hands-on experience is invaluable. Yet, despite the obvious merits of BAO training to the TSO workforce, at other airports TSOs state that while they are aware that there is a BAO assigned to their airport, the person does not conduct trainings for the TSO workforce.

Investment in Technology

Over the past few weeks there have been media articles referring to the leak of a classified TSA report that found a high percentage of simulated explosives and bomb parts that were missed by TSOs at three large airports. AFGE does not accept the leaked results as evidence that TSOs are doing anything other than a very good job protecting the flying public under very difficult conditions. The reported test results are not, in and of themselves, indicative of individual TSO or TSO workforce performance. The report should, however, be used as an early warning signal of problems that need to be resolved as quickly as possible.

The specific tests were covert where testers attempted to slip simulated explosives and bomb parts past passenger checkpoints. Unlike the covert tests of several years ago that involved the detection of fully assembled simulated bombs, these tests often involved very small components that are easily hidden in items that TSA has chosen not to ban. AFGE TSO members report that even in trainings where TSOs themselves disassembled a simulated explosive and hid its parts in carry-on baggage, they were unable to find the parts by sight alone. Simply put, TSOs cannot be expected to detect what the human eye cannot see.

The technology that would enable TSOs to detect potential weapons not readily apparent to the human eye is available, and is currently in use at three airports.

According to published reports, TSA has purchased 20 of the machines and plans to test them at other airports over the next few months. For years, in report after report, both GAO and the DHS Inspector General have called on TSA to invest in and deploy technology that will assist TSOs in performing their screening duties in response to the ever-changing efforts of determined terrorists. In a February 2007 report to Congress, GAO wrote, "TSA does not yet have a strategic plan to guide its efforts to acquire and deploy screening technolgies."[2] In an October follow-up discussion of the issue, GAO found that TSA "generally" did not achieve the goal of deploying checkpoint technologies to address vulnerabilities.[3]

In addition, it should be noted that TSA has put tremendous emphasis on "customer satisfaction". The customer could be either the carriers who want their planes to depart on schedule, or the flying public, who want to get through the screening checkpoint and on the way to their gate as quickly as possible. In fact, the goal of TSA (according to SAM) is to "provide the necessary level of aviation security and ensure that the average aviation security related delay experienced by passengers is minimized".[4] The reality is that there are many sources of delay to air travelers, including highway traffic, long lines at tickets counters and the sheer volume of passengers. All too often though, the blame for passenger delay is assigned to the checkpoint screening process. Although a goal of screening is to move passengers along as quickly as possible, it is not the only goal. TSOs report that they fear they may miss items that should receive additional scrutiny because they are under constant pressure to work quickly—at times, too quickly. TSA management should work with TSOs to test technology and develop protocols that keep the public safe while meeting the needs of passengers.

Lack of TSO Input

AFGE TSO members report that they have yet to feel that are a partner working with TSA to ensure aviation safety. According to the 2006 Federal Human Capital Survey, 54% of the TSA workforce, overwhelming comprised of TSOs stated that creativity and innovation are *not* rewarded at TSA and only 38% of the workforce believed they had "sufficient resources" to do their jobs. Half of TSA workers report they do not have "a feeling of personal empowerment" regarding work processes. Too often TSOs report they were laughed at by supervisors when they requested additional training. At many airports, speaking up about an alternative process or pointing out a problem was a certain path to retaliation, which could include either actual termination or harassing the worker until they quit. This attitude among TSA management runs counter to the mission of the agency by ignoring or discounting the input of over 43,000 TSOs on the frontlines of safety every day at 450 airports across the country.

TSOs have implemented SOPs that sometimes change on a daily basis. As the "face" of TSA, they have to listen to passenger complaints about removing their shoes, emptying containers, removing laptops from cases, as well as complaints from parents who don't want to take their babies out of strollers to proceed through the detectors. When a new SOP is communicated by management, TSOs must almost instantly grasp and implement it. Too often TSOs state that they receive no or incomplete feedback from supervisors as to whether their implementation is correct or not.

There should be a true and respectful discourse between TSA management and TSOs. No worker at DHS should be hesitant to point out a shortcoming that could impact public safety because they fear retaliation from management. This is a very real threat to the TSO workforce, because TSA refuses to be bound by the Office of Special Counsel's recommendations when TSOs are retaliated against for blowing the whistle on security breaches. TSOs do not have the right to appeal serious harmful personnel decisions to the Merit Systems Protection Board—even though their managers have that right. AFGE calls on Congress to pass H.R. 3212, a bill introduced by Representative Nita Lowey that would provide TSOs collective bargaining rights and workplace protections and ensure that they are treated the same as other workers at TSA.

The availability and level of training and deployment of technology is incredibly inconsistent among our nation's airports. Given the resources necessary to get the job done quickly and effectively, and with valuable input from the TSOs doing the tough job of keeping the public safe, TSA can further accomplish its mission.

---

[2] GAO–07–448T, Aviation Security: Progress Made in Systematic Planning to Guide Key Investment Decisions, but More Work Remains.

[3] GAO–08–139T, Aviation Security: DHS Has Made Progress in Securing the Commercial Aviation System, but Key Challenges Remain.

[4] GAO–07–299, Aviation Security: TSA's Staffing Allocation Model is Useful for Allocating Staff among Airports, but Its Assumptions Should be Systematically Reassessed.

This concludes my statement. I would be happy to take questions from the Subcommittee.

Ms. JACKSON LEE. And I now recognize Ms. Friend to summarize her statement for 5 minutes.

We welcome you. We thank you for your service.

And as I do that, let me acknowledge Congresswoman Ginny Brown-Waite of Florida, who has joined us, and a member of the committee.

Ms. Friend, thank you.

STATEMENT OF PATRICIA A. FRIEND, INTERNATIONAL PRESIDENT, ASSOCIATION OF FLIGHT ATTENDANTS-CWA, AFL–CIO

Ms. FRIEND. And thank you, Chairwoman Jackson Lee and members of the committee, for giving me this opportunity to testify today.

It was our members, flying partners and friends who were among the first victims to die at the hands of terrorists on September 11th, all while performing their duties with professionalism. Today flight attendants remain the only frontline first responders guaranteed to be in the cabin of every passenger aircraft.

Considering those facts, you would think that we would have been among the first to be given the tools and training to protect ourselves, our passengers and the aircraft. Unfortunately that is not the case. I hope that my testimony today will convince all members of this subcommittee that a glaring loophole in our aviation security remains, and that more must be done to close that dangerous loophole. While Congress and the administration have taken many steps to improve aviation security, flight attendants are still left in the passenger cabin with no meaningful training or tools.

In the immediate aftermath of the attacks on September 11th, it became clear that the flight attendant antihijacking and security training was outdated, inadequate and in major need of revision to reflect the current security threats. The report from DOT Secretary Mineta's Rapid Response Team called for a meaningful and comprehensive update for flight attendant security training, as did the staff report accompanying the 9/11 Commission report. We have repeatedly asked for the necessary improvements to our training, including basic self-defense maneuvers. We are not asking to be certified black belt martial arts experts, but simply a basic level of meaningful training to help protect ourselves, our passengers and slow down the next terrorist attack.

We also desperately need better training on crew communication and coordination among the three components of in-flight security: flight attendants, pilots and air marshals. Today security training provided to flight attendants consists of the advanced voluntary training program provided by TSA and a basic mandatory training provided by the airlines.

The TSA-developed advanced voluntary portion of flight attendant security training is conducted several times a year over 3 days at various community colleges around the country. The voluntary nature of the training requires a flight attendant to find 3 consecutive days off from work and to pay themselves for the necessary housing during these classes. AFA firmly believes that many of the

provisions of this voluntary program should be integral parts of a basic mandatory training program.

Currently the basic mandatory security training for flight attendants is provided directly by the airlines with little oversight by the TSA. Reports from our air safety health and security representatives indicate that security training has been systematically watered down year after year. A summary of reports on the status of flight attendant security training at a number of AFA-represented carriers is attached to my written testimony. A quick review will demonstrate the weakness of airline security training programs provided to flight attendants as first responders.

As well as a lack of the most basic meaningful security training for flight attendants, equipment for enhancing on-board aviation security is also lacking. The most basic necessity on board a passenger aircraft is the ability to communicate quickly, efficiently and clearly between the cabin and the flight deck crew. With pilots safely barricaded beyond their reinforced cockpit doors, and with instructions to limit exposure, it is crucial that a reliable and clear communication tool be provided for the aircraft crew to communicate with one another. Currently the only communication device available for cabin and flight deck crew is the aircraft interphone. This is the telephonelike device that I am sure you have all seen the flight attendants use on board aircraft. This device is unreliable for a number of reasons, but most critically access to an interphone may be blocked, or the interphone itself may be easily and quickly disabled.

The events of September 11th clearly demonstrated that a more reliable form of communication is needed. AFA, along with other unions representing flight attendants at major carriers in this country, have repeatedly called for a wireless communication device for flight attendants to use on board the aircraft. Such a device would provide flight attendants with the ability to notify pilots at the earliest possible moment of a problem.

Madam Chair and members of this subcommittee, it is unfortunate that I appear before you today 6 years after September 11th to tell you that while everything related to the experience of air transportation has changed, little has changed for the flight attendants' ability to protect you or themselves. The 9/11 Commission report highlighted numerous acts of bravery on that terrible day. It highlighted the heroic and professional acts performed by the many flight attendants on those four hijacked flights, even as they watched their flying partners brutally murdered. The report drew special attention to how the flight attendants on those flights acted in the best interest of their passengers and took action outside the scope of their training to do what they could to relay information and to protect those passengers and themselves. I can assure you that the flight attendants I know and represent would do the same thing again today when confronted with a similar situation. However, I am once again pleading with you to help make a repeat of that day a little less likely by giving us the tools and training that we need.

Thank you for giving me this opportunity to testify on behalf of the brave women and men who staff the passenger aircraft of the

U.S. aviation system. I look forward to answering any questions that you may have.

Ms. JACKSON LEE. Thank you very much, Ms. Friend.

[The statement of Ms. Friend follows:]

PREPARED STATEMENT OF PATRICIA A. FRIEND

NOVEMBER 1, 2007

Thank you Chairwoman Jackson-Lee, and the members of this Subcommittee, for giving me the opportunity to testify today. My name is Patricia Friend and I am the International President of the largest flight attendant union in the world, the Association of Flight Attendants—CWA (AFA–CWA). AFA–CWA represents flight attendants at 20 airlines with over 55,000 members. Our members work onboard airline operations from the largest, international flights to small, regional service in thousands of communities across this country. It was our members, flying partners and friends that were the first victims to die horrible, brutal deaths at the hands of terrorists on September 11th while performing their duties with professionalism. Today, flight attendants remain as the only front line first responders guaranteed to be in the cabin of every single passenger aircraft operating in this county. Considering those two facts, you'd think that we would have been among the first to be given the tools and training to protect ourselves, our passengers and the aircraft. Unfortunately, Congress and the Administration have failed to take the necessary steps to make that possible.

I hope that my testimony today will help convince all the members of this Subcommittee that a glaring loophole in our aviation security remains and that more must be done to close that dangerous loophole. I'm here to tell you that for the over 100,000 flight attendants in this country, very little has changed since the attacks of September 11th. While this Congress and the Administration have taken steps for airline pilots, who are now safely barricaded behind reinforced cockpit doors and are in some cases armed with guns, and air marshals are on a higher percentage of flights then before September 11th, flight attendants are left in the passenger cabin with no meaningful training or tools. This is an unacceptable situation and one which we, many aviation security experts and the 9–11 Commission have been urging a change to for well over six years now.

In the immediate aftermath of the attacks on September 11th, 2001, I was appointed by then Secretary of Transportation, Norman Mineta, to his Rapid Response Team for Aircraft Security, a group of industry experts assembled to recommend aircraft security improvements. The members of this team were appointed in order to bring our collective experience together to attempt to address what we viewed as the glaring loopholes that were exploited by the 9–11 terrorists. One of those identified loopholes was the inadequate and outdated training provided to flight attendants. The report for the Rapid Response Team called for a meaningful and comprehensive update for flight attendant security training to reflect the current threat environment, as did the staff report accompanying the 9–11 Commision.

It was clear that the flight attendant anti-hijacking and security training provided by the carriers was outdated, inadequate and in major need of revision to reflect the current security threats posed by terrorist attacks onboard aircraft. Previous training that called for flight attendants to be cooperative with terrorists that were hoping to land a plane somewhere to negotiate for the release of hostages was clearly no longer the situation flight attendants would face in another Al-Qaeda attack onboard an aircraft. The threat posed to flight attendants, passengers and the aircraft changed and our training needed to reflect the new reality.

What we have repeatedly asked for is to update our training to include a number of important facets. Among them are basic self defense maneuvers to allow for us to defend ourselves against a terrorist attack. We are not asking, as some have tried to portray it, to be certified black belt martial arts experts. We are simply asking for a basic level of meaningful training to protect ourselves and slow down any terrorist attack. Also included would be training on crew communication and coordination. Currently, there is no comprehensive training or explanation of what the three components of in-flight security—flight attendants, pilots and air marshals—are trained to do in case of an attack. Clearly, these three groups must be trained on how to work together as a team to be as effective as possible. Unfortunately, that is not happening.

Ever since 9–11, AFA–CWA has been engaged in aggressive and repeated legislative efforts to enact legislation to provide the meaningful training that we need. Unfortunately, our efforts have been thwarted by airline management—which is more

interested in the financial bottom line rather than meaningful security efforts—as well as refusal and outright stonewalling by federal agencies.

I have prepared an outline for the Subcommittee on our various legislative efforts since September 11th, 2001.

Air Transportation Security Act (ATSA)

Our first legislative efforts were undertaken in Congress during drafting and debate of the Air Transportation Security Act (ATSA) in the fall of 2001. The final legislation approved by Congress included provisions that required the FAA to update and improve flight attendant security training requirements. These provisions called on the FAA to require that air carrier flight attendant training programs be updated and changed to reflect the current security and hijacking situations that flight attendants may face onboard the aircraft. It was AFA–CWA's intention and belief by ensuring that the FAA approve these updated programs, all carriers across the industry would implement similar, if not identical, training programs.

However, in the immediate months after passage of ATSA it became abundantly clear that the security training programs being implemented by the carriers and approved by the FAA were not adequate or consistent. There was a wide variance in the type of training and the hours spent on the training. Some carriers were showing flight attendants a twenty minute video, while others were conducting two full days of mandatory, hands-on training. These discrepancies in the security training in the aviation system led to many flight attendants unprepared for any future terrorist attack onboard an aircraft. We have stated repeatedly that all flight attendants, regardless of the carrier employing them, must receive the same level of security training.

It was at this time that we began to urge Congress to change the requirements for flight attendant security training to include a provision that mandated a set number of hours for the security training. These mandates would have to be enforced so that all carriers would be required to provide the same level of adequate security training for all flight attendants. AFA–CWA still believes that this is the best requirement for training.

Arming Pilots Legislation

During the spring of 2002, as legislation began moving in the House and Senate that would allow pilots to carry fire arms, AFA–CWA asked that Congress mandate 28 hours of detailed flight attendant security training at all carriers, with the training requirements and guidelines to be developed by the Transportation Security Agency (TSA). In the House, AFA–CWA worked closely with Representative Steve Horn (R–CA) to introduce an amendment in the House Transportation and Infrastructure Committee to the Arming Pilots Legislation that would mandate 28 hours of detailed flight attendant security training. At the last minute, Representative Horn did not offer the amendment after discussions with the Chair and Ranking Member in the hope that language would be included in the final bill before reaching the House floor. Eventually, a provision was included in the final version that passed that House requiring TSA to develop detailed flight attendant security training requirements that must be followed by all carriers, but not mandating 28 hours specifically.

In the Senate, Senators Bob Smith (R–NH) and Barbara Boxer (D–CA) included AFA–CWA's ideal provisions mandating 28 hours of detailed flight attendant security training in their Arming Pilots Legislation. As the Senate debated amendments to the Homeland Security Act on September 5th of 2002, we were successful in convincing a majority of Senators to support the amendment and succeeded in including the provisions in the Homeland Security Act.

Homeland Security Act

The House version of Homeland Security did not include provisions on arming pilots or flight attendant security training. While the bill was being finalized in the Homeland Security Act Conference Committee, AFA–CWA urged the Committee to support the Senate version of the language, but we were ultimately unsuccessful in having the mandated 28 hours of training included. The final legislation did include language that would require TSA to issue a rule mandating a set number of hours for extensively detailed flight attendant security training that must be implemented by all carriers and mandatory for all flight attendants.

While not completely satisfied with the final language, we began to work closely with TSA and those developing the training curriculum and guidelines in order to guarantee that the training requirements and the final rule issued by the TSA would be as strong and comprehensive as possible.

Airline Management Efforts to Kill Flight Attendant Security Training

Airline management has been strongly opposed to any efforts that would require them to abide by any industry wide training standards or a firm requirement on the number of hours required for training. To them, it has not been an issue of security, but an issue of bottom line profit. They have fought AFA–CWA every step of the way and have even attempted a number of back door efforts to completely gut requirements for flight attendant security training.

In the spring of 2003, they attempted to insert a provision into the Omnibus Appropriations Act that would make any flight attendant security training required by TSA voluntary. They had also worked consistently to legislate that any flight attendant security training be made voluntary, make the flight attendants pay for the training themselves and prevent industry wide standards for the security training or eliminate it completely.

Vision 100—FAA Reauthorization

In 2003, as the House worked on its version of the Vision—100 FAA Reauthorization, the carriers continued in their efforts to gut flight attendant security training. Early in the process, AFA–CWA was approached by certain carriers about possibly reaching a compromise on the issue that could be acceptable to all. It was abundantly clear to flight attendant labor unions that we could either negotiate with the committee on language that we could live with or take our chances with airline management forcing through their preferred language. Regardless of our support for the current law, it was clear that the Congressional leadership of the majority were intending to enact changes to flight attendant security training, at the request of airline management.

In the end, the final language included in the House FAA Reauthorization created a two tier approach to training. It created an advanced, voluntary training program and a basic, mandatory level of security training with the requirement that TSA must develop firm and specific guidelines for that training. It was our understanding that this compromise was a settled issue. Unfortunately, at the last minute, Continental Airlines went to Republican House Leader Tom DeLay and had him change one word in the security training provisions. He had the provision that said "TSA **shall** issue guidelines" changed to "TSA may issue guidelines". By changing this one word, he took away the ability to force TSA to issue these guidelines. TSA, which has proven to be under the pressure of the carriers, would now not be required or mandated to issue meaningful guidelines for crucial, mandatory flight attendant security training.

Since enactment of that legislation, AFA–CWA has pursued various efforts to improve upon our security training. Unfortunately, we have been unsuccessful.

Current Status of Flight Attendant Security Training Programs

Today, training provided to flight attendants remains unsatisfactory. It consists of the advanced, voluntary training program provided by TSA and basic mandatory training provided by the airlines themselves.

Advanced, voluntary training

Currently, the TSA has developed the advanced, voluntary portion of flight attendant security training. The training is conducted several times a year over three days at various community colleges around the country and focus on self defense training. At times, TSA has been slow in providing information on class locations and dates, depressing turnout. It has also become increasingly difficult for our members to attend the training as it has become harder for them to find three consecutive days to take off from work. Also, with the recent rounds of bankruptcies in the airline industry and the resulting dramatic pay cuts, our members have found it difficult to pay for the necessary housing during these classes. Questions remain about the effectiveness of this training when it does not include a yearly recurrent training. This is a one time training that does not require a yearly "refresher" course. Further, AFA–CWA firmly believes that many of the provisions of this voluntary program should be integral parts of a basic, mandatory training program.

Basic, mandatory training

At this time, the basic mandatory security training for flight attendants is provided directly by the airlines themselves, with little oversight by the TSA. While Congress established the TSA to develop and oversee transportation security programs, according to the September 2005 Government Accountability Office (GAO) report to Congress on flight attendant security training, TSA believes it is the individual air carriers themselves who are responsible for establishing performance goals for these training programs. Unfortunately, TSA's inability to carry out its most basic oversight capabilities has resulted in a further watering down of flight attendant security training programs over the past several years.

In fact, reports from our Air Safety, Health and Security representatives at AFA–CWA represented carriers of all sizes indicate that security training has continually been watered down year after year. In fact, one of our members recently reported that instead of spending time on required security training, the airline instructor released the students in order to "take an early lunch", neglecting to cover the required program. I have attached a summary of reports from our representatives on a number of AFA–CWA represented carriers, you can see how the training is again as varied and random as that which existed prior to September 11th.

The 2005 GAO report goes on to state that TSA has failed in its basic requirement to provide overall strategic goals for the carriers or to develop a framework from which to establish goals for the training. While TSA told the GAO that they planed on completing work on detailed guidance for airlines two years ago, to our knowledge, they have continued to fail in this most basic requirement.

Furthermore, TSA has been given the ability to periodically review and audit airline training programs. It is unclear how frequently TSA is actually undertaking this requirement. In fact, as the September 2005 GAO report stated, "although TSA officials stated that TSA inspectors reviewed all 84 air carriers' revised security training curriculums in response to January 2002 guidance and the corresponding standards, TSA was only able to provide us documentation related to 11 reviews."

Also, the Vision 100 FAA Reauthorization included a provision that required the TSA to consider complaints from flight attendants when determining when to conduct a review and audit of a carrier's security training program. TSA representatives told the GAO that they "were not aware of any instances in which crew members had complained to TSA" about the training programs. I can attest to the fact that this is not accurate. AFA–CWA members have written TSA to complain about the watering down and inadequacies of their training programs. Either TSA officials do not read their mail, or they were not truthful with GAO investigators.

The September 2005 GAO report is full of promises from the TSA to develop reporting guidelines, databases for the tracking of carrier training programs, a handbook to document procedures for TSA inspectors and reorganizing inspection staff into a newly created Office of Compliance. I urge this Committee to conduct the proper oversight to see if TSA has truly and completely followed through with their promises to the GAO over two years ago. While taking these steps still leaves the current security training woefully inadequate, it could help provide a level of consistency that is currently lacking in the industry.

I regret to inform the members of this Subcommittee that due to TSA inaction and lack of oversight, airline managements' desire to streamline and cut training programs and lack of—to date—Congressional oversight, flight attendant security training programs are no more effective today as they were prior to September 11th.

Lack of Equipment to Enhance Aviation Security in the Aircraft Cabin

As well as a lack of the most basic, meaningful security training for flight attendants, equipment for enhancing onboard aviation security is currently lacking. The most basic necessity onboard a passenger aircraft is the ability to communicate quickly, efficiently and clearly between the cabin and flight deck crew. With pilots safely barricaded behind their reinforced cockpit doors, and with instructions to limit exposure, it is crucial that a reliable and clear communication tool be provided for the aircraft crew to communicate with one another in an emergency situation.

Currently, the only communication device available for cabin and flight deck crew is the aircraft interphone. This is the telephone device that I'm sure you've all seen the flight attendants onboard the aircraft use to make announcements and to communicate with the cockpit. This device is inconvenient for a number of reasons. First, an inoperable interphone is not a reason to prevent an aircraft from departing for a scheduled flight. Second, the interphone is located in the galleys of the aircraft—all the way in the aft or in the front—making it very difficult to run to in an emergency situation if flight attendants are located throughout the cabin of the aircraft.

It should also be noted that when various federal agencies conducted a mock terrorist attack onboard an aircraft in June of 2005, referred to as "Operation Atlas", one of the first things that the mock terrorists did was to cut the phone cord on the aft interphone, thereby restricting communication between the cabin and cockpit. Many crucial minutes passed before the cockpit crewmembers were even aware that anything had happened, giving the terrorists plenty of time to kill and injure various crewmembers and passengers. While this was a mere "mock" hijacking, such a possibility exists today.

AFA–CWA, along with other unions representing flight attendants at major carriers in this country have repeatedly called for a cost effective, wireless communication device for flight attendants to use onboard the aircraft. Such a device would

provide flight attendants with the ability to notify pilots at the earliest possible moment of a problem. The technology is available today and has even being factored into the designs on the newer aircraft coming off the assembly lines at Boeing and Airbus. There are several different vendors in this country that have prepared just such a cost effective and functional device that could easily be integrated into the aircraft operating systems and could be installed on all U.S. commercial aircraft in a relatively short period of time. AFA–CWA believes that it is well past time that hands-free, discreet, wireless devices should be made mandatory for all flight attendants.

The need for such a device is not a new one that has only emerged post 9–11. In fact, in 1999, the White House directed the FAA to establish the Commercial Aviation Safety Team (CAST) to investigate numerous turbulence injuries that were occurring onboard aircraft. That year, the CAST Committee began working on a bi-directional wireless communications system for pilots and flight attendants. The system was needed because at times of spur-of-the-moment turbulence, the pilots could not ensure that flight attendants would hear a public address warning over the cabin intercom. In addition, numerous cases of flight attendant and passenger injuries due to turbulence could not be communicated to the pilots because the flight attendants were unconscious on the floor with no means of communicating. Studies reviewed by CAST showed that wireless notification would result in huge savings for air carriers with fewer flight attendant on-duty injuries. The business case based on this is available.

The events of 9–11 clearly demonstrated that a more reliable form of communication, other than cabin interphones, is needed. Other methods of determining the cabin status such as video cameras have been tested but are laced with problems and concerns about their usage. A wireless system allows for integration of the air marshals and provides a compromise to the countries that do not want lethal weapons or air marshals onboard the aircraft.

In fact, Congress itself has recognized the possibility that this technology presents. The Aviation Transportation Security Act (ATSA) directed the FAA to "revise procedures" for communicating between the cockpit and aircraft cabin. Then in March 2002, the International Civil Aviation Organization (ICAO), recommended that all international carriers provide flight attendants with a discreet, wireless communication device. In December 2002, the Homeland Security Act gave the TSA the ability to require discreet, wireless communication devices for flight attendants. And the Intelligence Reform and Terrorism Prevention Act of 2004 included the requirement that the TSA conduct a study on the technology and ability to install such a wireless communication system.

Unfortunately, as with our training, neither TSA, nor the FAA have taken any actions to try and provide such a communications system, even after repeated requests from Congress that something be done. In fact, the FAA has taken the position that there is no need for additional technology or communication devices onboard the aircraft. They believe that teaching flight attendants and pilots a secret knock, followed by a code word is sufficient enough method to communicate that an attack of some sort is taking place. I am not joking, even though I sincerely wish I was.

Madame Chair and members of this Subcommittee, it is unfortunate that I appear before you today, six years after September 11th, 2001—six years after our colleagues were among the very first victims on that day—to tell you that little has changed since that day. I wish I could tell you differently, but I can't. We have tried repeatedly to get Congress, the TSA and our employers to take the action necessary. Those efforts have been repeatedly thwarted. While air marshals are on more flights and pilots are barricaded behind reinforced doors and provided with lethal weapons to protect themselves those most at risk, and those most able to act in the aircraft cabin to defend their passengers and the aircraft, have been provided little tools. I want to ask Congress—even if a cockpit is protected and the pilots land the aircraft successfully, while everyone in the passenger cabin is dead, have the terrorists still not achieved their goal to wreak havoc and bring terror back into our lives?

The 9–11 Commission report highlighted numerous acts of bravery on that terrible day. It highlighted the heroic and professional acts performed by the many flight attendants on those four hijacked flights even in the light of seeing their devoted flying partners brutally murdered. It drew special attention to how the flight attendants on those flights acted in the best interests of their passengers and "took action outside the scope of their training" to do what they could to relay information and to protect those passengers and themselves. I can assure you that the flight attendants I know and represent would do the same thing again today when confronted with such a situation. However, I beg you to please help make a similar repeat of that day a little less likely, by giving us the tools and training we need.

Thank you for having the opportunity to testify today and I look forward to answering any questions that you may have.

Ms. JACKSON LEE. And if I might, as I introduce, thank you for your important testimony, just to indicate that anyone who focused on 9/11, as we all have done, and certainly we respect all of the law enforcement and frontliners in transportation security, allow me to acknowledge in particular the flight attendants for the role that will maybe go untold on 9/11 as they continue to put passengers first. And we thank them very much for all that they have done.

I would like to now yield to and recognize Captain Hesselbein to summarize his statement for 5 minutes, and we thank him very much.

Welcome, Captain Hesselbein.

STATEMENT OF ROBERT HESSELBEIN, CHAIRMAN, NATIONAL SECURITY COMMITTEE, AIR LINE PILOTS ASSOCIATION, INTERNATIONAL

Mr. HESSELBEIN. Thank you. And good afternoon, Madam Chairwoman and distinguished members of the subcommittee. On behalf of the 60,000 ALPA members who fly for 42 airlines in the United States and Canada, I want to thank you for this opportunity to provide a frontline perspective on aviation security training and equipment needs.

For such a broad topic, I have decided to narrow my remarks to just two of the association's security priorities. I would like to address the training and support gaps in the Federal Flight Deck Officer Program, and also the need for secondary barriers and procedures to protect our flight decks.

Let us start with the Federal Flight Deck Officer Program, or as we call it the FFDO Program. The first class of 44 FFDOs graduated from training in April 2003. Since then many, many thousands of airline pilots have been trained, deputized and now serve as Federal flight deck officers. But there are several things that are hampering the recruitment and retention of FFDOs. They must often risk discipline by their employers to attend training. They must pay all out-of-pocket expenses to attend training as well. And to practice and requalify, they have to spend their own money, and then they must perform their duties with no postgraduate mentoring and no minimal supervision. They are expected to accomplish their duties and succeed in their assigned missions, but they do it with a fraction of the support structure enjoyed by other Federal law enforcement officers.

Many employers will not permit pilots to take unpaid leave to attend FFDO training. Unlike military leave, there are no legal devices that require employers to allow their pilots to leave for required training. In fact, some airlines create obstacles for pilots to attend this valuable training.

After graduating from basic training for which they personally pay up to $500 in housing, meals and transportation expenses to attend, an FFDO is deployed on mission status without the guidance of a field training officer or frontline supervisor. All that the FFDO has for support is a TSA phone number to call if any issues

arise, access to a protected Web site for routine scheduling, and they also can access a Web site for administrative information.

Furthermore, there is no partner system in place to mentor incoming FFDOs, and no routine supervised training beyond a 6-month proficiency demonstration until their third year of mission status. At that point they are provided with 2 days of recurrent training.

Speaking of which, the Federal Air Marshals Service announced that as of April 25, 2007, all FFDOs must attend a 2-day recurrent training event in Atlantic City, New Jersey, at a certain interval within their FFDO career. Because of the very limited training dates and locations, pilots must often travel hundreds, if not thousands, of miles to attend, again at their own expense. This function may cost pilots upwards of $800.

In a time of significantly reduced pilot salaries and terminated pension plans, we are concerned that the FFDO Program's attrition rate will grow, and fewer pilots will make the personal sacrifices needed to keep the program alive. One solution is to add more training locations and use current Federal air marshal facilities for their training.

We believe Congress can take a few simple steps to ensure that FFDOs remain an effective force in protecting our skies. First of all, enact legislation that gives FFDO trainees the same leave rights as those citizens performing military service. Second, we must ensure that pilots who enter the system have ongoing and frequent access to standardized training that includes protocols, procedures and training scenarios that coordinate with our Federal air marshal counterparts and, especially, reimburse the FFDOs for their reasonable out-of-pocket training and travel costs.

Speaking of cost-effective measures, ALPA believes that the flight deck's secondary barrier and associated procedures will provide the biggest bang for the taxpayer bucks in terms of aviation security on the flight deck. To that end ALPA has worked closely with Congressman Steve Israel on the development of a bill, H.R. 3925, that would mandate the installation of secondary barriers in all Part 121 aircraft.

While the reinforced door is a vital element in flight deck protection, it is not fully sufficient to protect the flight deck from a well-coordinated, efficient assault executed when the door is open. An inexpensive secondary barrier, along with access procedures, will ensure that door transitions are made safely, securely and in minimal time. Importantly, two U.S. major airlines have already developed and installed these secondary barriers on their airplanes, and others seek agreed-upon design standards for their manufacturing installation as well.

The industry seeks standardized procedures to complement these use of secondary barriers to complement the wall fortifications. The few seconds that a secondary barrier will buy during a hijacking event are worth their weight in gold if they prevent hijackings. The barriers are especially needed on all cargo aircraft as well, which do not even have a flight deck door between the cargo and the crew.

In summary, all FFDOs must be effectively trained and supported to remain a successful part of the security process. Inexpen-

sive secondary barriers that have a high benefit for a very low cost should be considered and installed. We urge Congress to support both of these initiatives.

Thank you very much, and I would be happy to answer any of your questions.

[The statement of Mr. Hesselbein follows:]

PREPARED STATEMENT OF CAPT. ROBERT HESSELBEIN

NOVEMBER 1, 2007

Good afternoon. I am Bob Hesselbein, Chairman of the National Security Committee of the Air Line Pilots Association, International (ALPA). ALPA is the world's largest pilot union, representing more than 60,000 pilots who fly for 41 airlines in the U.S. and Canada. ALPA was founded in 1931 and our motto since its beginning is "Schedule with Safety." We are pleased to have been asked to testify today on the important subject of human resources and equipment as used to enhance aviation security.

There are obviously a great many subjects that could be addressed within this general topic, but today I would like to focus on just two: Federal Flight Deck Officer (FFDO) training and support needs, and secondary barriers on flight decks.

Federal Flight Deck Officer Program

ALPA was the first organization to call for the creation of the Federal Flight Deck Officer (FFDO) program, which became a reality when the Arming Pilots Against Terrorism Act (APATA) was enacted as part of the Homeland Security Act of 2002.

The first class of 44 Federal Flight Deck Officers graduated from training in April 2003. Since then, thousands more have joined their ranks and are recognized as key components in the U.S. government's layered approach to protecting the aviation domain. Because the majority of these federal law enforcement officers are ALPA members, the Association has a vested interest in the integrity and viability of the program and remains engaged in a close working relationship with the Transportation Security Administration (TSA) and the Federal Air Marshal Service (FAMS) to ensure the program's continued success.

The FFDO program is unique in that it capitalizes on the willingness of volunteer candidates to protect a critical component of the nation's infrastructure. In order to become an FFDO, a pilot must successfully pass background, psychological and physical requirement vetting, and then complete a rigorous initial training curriculum at the Federal Law Enforcement Training Center (FLETC) in Artesia, NM. Upon so doing, the pilot is deputized as a federal law enforcement officer and, under color of federal law, is empowered to use lethal force to protect the flight decks of passenger and all-cargo transport category aircraft. No other such program exists within the federal law enforcement domain.

From the outset of our support for the FFDO program, we have emphasized that the initiative must select, train and deputize qualified candidates who are chosen from the airline pilot population. We applaud TSA's significant efforts to develop and deploy the FFDO program, and the FAMS' contributions in maintaining and managing it. These successes notwithstanding however, it must be noted that FFDOs are not provided with post-basic training opportunities beyond the need to demonstrate semi-annual weapons proficiency and a brief two-day refresher course after three years of duty.

ALPA has brought this inadequacy to the attention of the TSA/FAMS upon numerous occasions. Although armed pilots have shown tremendous professionalism in the performance of their duties and provide the most wide-spread armed federal security coverage in United States airspace, we remain concerned that their training and mentoring falls short of what other federal officers receive to accomplish their respective missions. It is clear that no other federal law enforcement officers are expected to succeed in their assigned missions without a support structure which includes post-basic-training mentoring and ongoing training.

As an example of this shortcoming, the FFDO's duty to protect the flight deck clearly supports the mission of the Federal Air Marshal Service. However, armed pilots are not trained to work in coordination with FAMs and are generally unprepared to deal with an onboard security event requiring FAM intervention. Determining how to handle an attempted hijacking should not happen at the moment it occurs, but rather during training events on the ground. Response protocols, procedures, and training scenarios should be coordinated between FFDOs and FAMs in advance—the middle of a crisis is not the time to make introductions and determine

each other's unique roles. The federal government conducts interagency crisis management exercises on a regular basis. It is only reasonable, therefore, that armed FFDOs should know what to expect from FAMS in the event of an attempted assault on the cockpit, and what the FAMS will expect of them.

FFDOs, by the very nature of their work, operate individually and with little direct supervision. Nearly all communication between them and FAMS program managers is accomplished by secure e-mails which generally incorporate basic advisories or scheduling details. Clearly, this missed opportunity for distance learning, information sharing and mentoring is a program shortcoming. FFDOs should be provided mission-related educational materials using secured-access libraries. In addition, training opportunities should be provided at local FAMS field offices.

Another significant issue which serves as a deterrent to pilot participation in the program relates to the need to compensate volunteer FFDOs for out-of-pocket expenses that they incur during initial, re-qualification and recurrent training events. These costs include hotel, meal, travel, ammunition and incidentals, which can add up to hundreds of dollars for an individual pilot. ALPA believes the government should assist the FFDOs by reimbursing them for such expenses for the following reasons:

• *The program is a key component of our nation's layered aviation security system.* Its value has been attested to by multiple components of the federal government, to include the Department of Homeland Security, the Transportation Security Administration and the Federal Air Marshal Service. Because global intelligence efforts continue to indicate that aviation remains a key target for terrorism, this reality must not be underestimated. The program was overwhelmingly approved by Congress because of its demonstrated need and because of the responsible vision that was articulated for developing and deploying it.

The presence of FFDOs on commercial flights is a component of the system utilized to schedule Federal Air Marshal flight coverage and by the North American Air Defense Command (NORAD) in the decision-making matrix related to handling security events involving transport category aircraft. FFDOs are tracked by the government not only when they are piloting aircraft, but also when they are in transit, while deadheading, or commuting in the aviation domain in order to utilize all resources to best advantage.

• *Initial training and re-qualification costs deter FFDO program applications.* FFDOs frequently incur significant out-of-pocket expenses to attend basic and re-qualification training. Average travel, food and lodging costs incurred for basic training vary from $300 to $500. Additionally, mandatory twice-yearly firearms re-qualification costs an average of $75 per event for most FFDOs. However, because of a lack of re-qualification sites in Alaska and Hawaii, FFDOs domiciled in those states must travel to the continental U.S. twice yearly to fulfill training requirements, which may require the pilot to use several days of personal time. As a result, these FFDOs incur lodging and food expenses averaging $150 per re-qualification event. Because FFDOs are not reimbursed for such costs, application rates are negatively impacted. Re-qualification sites are needed in the states of Hawaii and Alaska.

• *Recurrent training requirements have increased FFDOs' costs.* After three years of service, FFDOs must attend a two-day recurrent training event in Atlantic City, NJ. For most FFDOs, attendance at two full days of training requires a commitment of four days of their time, plus associated travel, hotel and meal costs estimated at $800. The FFDO program will likely lose some current participants and potential candidates as a direct result of the fact that only one training site will be used for this purpose. In times of significantly reduced pilot salaries, terminated pensions, and difficulty in obtaining leave for training, the impact on FFDOs is significant. To alleviate this problem, additional, strategically located recurrent training sites are needed. The FAMS has indicated its awareness of this problem, and should be provided with sufficient resources to address it.

• *The FFDO program is efficient and cost-effective.* It supplements the FAMS and provides a high degree of deterrence at a small cost to the US government and taxpayers. The government should recognize the value that is derived from the program and do all within its power to support and grow it, rather than letting it languish and diminish.

• *FFDOs have no external means for raising funds.* Unlike other individuals who volunteer to assist a government entity by performing a dangerous duty (e.g., volunteer firefighters), FFDOs have no external means of raising funds to cover their personal expenses. They are not allowed to hold fundraisers, solicit funds, or even identify themselves to the public.

• *Financial demands are causing FFDOs to reconsider their participation in the program.* FFDOs are *volunteers* who provide a reliable level of security for the domestic aviation industry at no cost to air carriers and at minimal cost to the government. By their own choice, they subject themselves to significant government regulation, supervision, personal expense, liability and risk. The more demands for personal sacrifice they are subjected to, the greater the risk that their willingness to participate will diminish or evaporate. This fact is now being demonstrated as FFDOs learn that they must pay significantly in terms of dollars and personal time to attend recurrent training. Even before the announcement was made about the new recurrent training requirement, some FFDOs had reached a point of departure from the program because the personal cost in time and money had become too great.

Clearly, Congress did not intend for the FFDO program to mature in a fashion that would cause current FFDOs to decline further participation, or to discourage prospective candidates from applying. However, the program has reached this stage because some pilots are simply unwilling to fund this layer of national security from their own pockets any longer.

FFDOs provide a direct service to the nation and the aviation industry. The government should recognize the special nature of this program and ensure its ongoing viability by funding personal costs incurred by FFDOs related to training.

The Association has worked continuously to suggest areas of additional "fine tuning" to the FFDO program since its inception, initially with TSA and more recently with the Federal Air Marshal Service (FAMS) since it assimilated the program two years ago. We have outlined in a white paper on the FFDO program 12 specific areas in which the program may be enhanced. We recommend that Congress legislate these improvements.

Secondary Barriers

Airplane cockpits are vulnerable to breach and seizure during fortified cockpit door opening and crewmember transitions during flight. Flight and cabin crewmembers are not rigorously trained, however, to prepare and protect the integrity of the flight deck during the door opening and closing process, and what training is provided is not standardized between airlines. To remedy this shortcoming, ALPA is actively promoting the installation of flight deck secondary barriers to protect against an attack. These barriers, which have already been installed on some aircraft by two major airlines, are lightweight devices mounted on the passenger cabin side of the flight deck door and serve to deter individuals from congregating near the door, attempting to open the door, and help to identify those who may intend harm to the flight. The barrier is not intended to prevent access to the flight deck door, but it does provide a delay which helps give the flight and cabin crew invaluable seconds to react to a threat. The barrier is used in conjunction with the proper training of crewmembers and a standardization of procedures and protocols to ensure full security.

Reinforced, or fortified, cockpit doors have added a valuable level of protection to airliner flight decks never before provided. A secondary barrier, accompanied by standardized procedures and protocols for protecting the cockpit door during those times it must be opened in flight, would significantly augment the fortified door and add an important layer of security to prevent hostile takeover of the cockpit.

ALPA has expressed and coordinated its support of a secondary barrier with ALPA member airlines, other associations and non-member airlines, and with TSA and the FAA. We have found there to be a consensus among all those contacted that the secondary barrier is a valid proposal and that such a security enhancement would bring added value to aviation security at a reasonable cost.

ALPA has worked closely with Congressman Steve Israel (D–NY) on the development of a bill, HR 3925, that would mandate the installation of secondary barriers on all Part 121 aircraft. ALPA fully supports this bill and calls on Congress to enact it promptly.

In July of this year, ALPA published a white paper titled *Secondary Flight Barriers and Flight Deck Access Procedures, A Call for Action* which provides further details about this important equipment. That paper urges Congress, FAA, TSA, and industry to support secondary flight deck barriers and provide accompanying flight deck access procedures on all airliners by January 1, 2010. These barriers should be built to a standard that will delay an attack on the cockpit by at least five (5) seconds, thereby enabling crewmembers to close and secure the reinforced cockpit door.

Again, we appreciate the opportunity to testify today and would be pleased to address any questions.

[For additional see Appendix.]

Ms. JACKSON LEE. Let me thank you and all the witnesses for their testimony.

At this time I remind each Member that he or she will have 5 minutes to question panel one. I now recognize— which is the panel for today. I now recognize myself for questions.

Let me just have this question for each of you. You have made and provided this committee with a litany of concerns, which is why we are having this particular hearing and why I noted the absence of the air traffic controllers, who I believe are very much a part of helping to secure America. But the question that I want to ask each of you is that the various need for improvement, the various issues that you have raised that suggest a need for improvement, in your answers tell me whether or not you feel that this impacts on the security of America? And that is why we are here.

And so, Mr. Gage, you mentioned the lack of relevant training, the low-grade nature of the training, and the fact that technology is not used at the level that it should. And I think a point that is very stark, the 19 percent attrition rate. So let me ask the question on how all of that, from your perspective, impacts on the security of the aviation traveling public.

Mr. GAGE. I think it impacts on it very negatively, and I think these are all choices that TSA has made. When training is old, it doesn't keep up with really the issues at the workplace, that training is useless; when training is inconsistently applied, when there is not enough staff. There was one of our screeners who asked why he hadn't been trained in a month, his training he is supposed to receive every week, and the supervisor basically just laughed. And it shows that the pressures that the TSA puts the workers as well as the supervisors under, it just does not take into account the risks. And I think it is a choice that TSA made. Even in technology, I don't believe they have stepped out on technology that could be most effective.

So I think all these things add up to a workplace where instead of having good, solid workers who really see what their job is about and how important it is to the country, we have a revolving door. And I think that is probably the result of many of these choices that TSA has made.

Ms. JACKSON LEE. Thank you very much.

You are remembering in your testimony, as you mentioned, the leak results of the covert testing on simulated bombs and bomb parts. Would you just quickly tell me what you think TSA could have done better to prepare the TSOs for future tasks? And with that I am going to submit into the record a statement by the Federal Law Enforcement Officers Association that recounts a number of incidents regarding the lack of detecting bomb material coming through the checkpoint.

Mr. GAGE. I think clearly that is a matter of technology. In my statement it said you can't hold a screener responsible for what he can't see with the current technology that is employed. And as I said, too, that even when our screeners became innovative and were placing components of an explosive device, very, very difficult to pick up and align at a checkpoint or even in the baggage area. So I think on that, technology clearly has to be purchased, has to be employed and has to meet the threat.

Ms. JACKSON LEE. Thank you.

Ms. Friend, your membership are clearly on the frontline as well. And you indicated meaningful tools and the idea of training. For example, are you concerned that defense courses for flight attendants will place a burden on them to engage physically? Also, the pure communication tool, and I agree with you, it is clear that that one communication system is very vulnerable. Does the plight of your flight attendants today impact on security, and what is the most crucial need that you have today for flight attendants?

Ms. FRIEND. Thank you.

The aviation security system that we have developed over the past 6 years is a layered approach starting from the no-fly list to the security checkpoint to the reinforced cockpit doors, the FFDO Program. But the reality is when those layers fail, there is no one in the cabin of that aircraft except for the flight attendant, and as it should be.

I don't mean to be critical in this response, but the pilots, armed or not, are not coming out of that cockpit to help, and they shouldn't, because it is critical that we protect the cockpit. But those of us who have become the last line of defense, the human shield, if you will, against the invasion of the cockpit, have no training on how we can best protect ourselves in a situation like that. We have—we are missing the most basic of tools to let the cockpit know that there is a serious security breach in the cabin of the aircraft. The only hope for any of us in that aircraft is to get that airplane safely on the ground. The sooner the flight deck crew knows that there has been a breach and that they must get the aircraft on the ground, the sooner that we can all be rescued. In the meantime, we are at the mercy of the individuals who have managed to breach this layer of security.

Ms. JACKSON LEE. You think the state of affairs impacts on the security of the passengers?

Ms. FRIEND. Absolutely, absolutely. Without being overly dramatic, we may, in fact, with a barricaded cockpit door get that aircraft on the ground. The question is how many fatalities will exist in the back of the aircraft by that time.

Ms. JACKSON LEE. Let me just say that we are writing legislation, this committee is, in addressing that question. Let me thank you for your testimony.

And it is my pleasure now to yield 5 minutes to the distinguished gentleman from California Mr. Lungren.

Mr. LUNGREN. Thank you very much, and I thank the three witnesses for appearing before us and their very interesting testimony.

Let me ask you this. We have problems. We are not perfect. We need to do more. But I would just ask the three of you, we have not had another instance since 9/11 in which someone has captured an aircraft and done what the terrorists did. Is that, in your judgment, pure happenstance, or are some of the things that we have done since then, have they been effective; and if they have been effective, which things that we have done with respect to your employees do you think have been effective?

Mr. Gage.

Mr. GAGE. No, I don't think it is happenstance. I think that they are doing a very good job. I think everybody takes their job seri-

ously. But at the same time, Congressman, I think that it could be more coordinated. I think that the training can be more consistently applied. I think that you shouldn't short-cut training, especially—for instance, a new standard operating procedure may come out, and the employee has no time to review it, has no time to see it, yet he is tested on it. And it just seems that—I think the training aspect, and to make this a more professional workforce, would go a long way to reducing the turnover, which something has to be done about the turnover and the way these people are treated on the job without any voice at work and with a performance system that just doesn't encourage creativity or innovation or even—or reward, I think, good solid work.

Mr. LUNGREN. And a system of feedback in which the ideas of the frontline people is actually taken into serious consideration.

Mr. GAGE. That is true.

Mr. LUNGREN. Let me ask you this. In terms of training, if you do testing properly, if you use testing as a training tool, that can be very effective. That is, if you have continual training in which you find where there are some holes, and then you use that to point out to your employees where, in fact, the shortcomings were, and use that to reenforce the training either that they have or new training that they are then receiving, it actually is part of the training as opposed to just a gotcha program?

Mr. GAGE. I don't disagree with that at all. But, for instance, our screeners are subjected to—one part of their certification is a contractor, a Lockheed—Martin. I don't know what they are doing there. But they come in, and our people are supposed to pat them down, and if they touch too softly, or if they touch too hard, something goes to their supervisor which affects their evaluations, affects their certification. They have no say in it. They don't even know what this person is looking for. But it is a negative. It is not really training there. It is totally gotcha.

Mr. LUNGREN. I understand what you are saying.

Ms. Friend, the question about what has been effective, if anything has been effective, from your standpoint and the standpoint of the people you represent.

Ms. FRIEND. Clearly, as I said, we have set up this aviation security that is layered, and so far it is working. But we do know that those who would recreate an event as spectacular as that of September 11 are constantly probing the system. So the fact that they haven't yet found a weakness that they can exploit on a particular day doesn't mean that they are going to stop trying.

Mr. LUNGREN. Let me ask something on that, and that is that we know that the American people today would react differently than they would have before 9/11, because beforehand we were told, sit in your seats, don't do anything, you will be in for a long ride, but eventually they just want to go somewhere. Now we know they want to use the aircraft as an instrument of destruction. So you have your passengers who are going to react differently and aid attendants if they need it. Is that taken into account in terms of the training?

Ms. FRIEND. No, it is not. And I say that simply because we have not seen incorporated into our training a module or a portion on how do you manage that reaction. I mean, it is a question, I sup-

pose, of crowd control. I mean, you don't want an out-of-ontrol mob. And you will have some passengers on board who will want to help, so help me understand how best to use that willingness to help, and don't expect me to just stand back and let the mob take over.

Mr. LUNGREN. Mr. Hesselbein, in terms of the pilots who are the flight deck officers that we have in the program now, do they receive training about how they exit the cockpit, when they exit the cockpit, what they look for, how they use—where they place their weapon during that period of time, all those sorts of things? Is it that detailed such that they feel confident when they are taking their breaks and where they place the weapon and when they are supposed to use it and all that sort of stuff?

Mr. HESSELBEIN. Congressman, without getting into the——

Mr. LUNGREN. I don't want you to get into the absolute details. I am asking you is it that comprehensive so that we would have some confidence in these officers?

Mr. HESSELBEIN. We have great confidence in the training the officers get in the understanding that their jurisdiction is a small flight deck area, and they are trained to protect that area and that space alone, and they are very well trained.

I would like to address just a couple other comments that were thrown out as well from other members of the board, and I would like to reinforce that. First of all, there have been almost 60 hijackings since 9/11 across the world, so hijackings will continue. And the success of 19 individuals in 1 morning is certainly a motivator for those who choose to do great damage to attempt to do it again despite our effort.

In regards to passenger responses of Flight 93, we cannot presume that all passengers will have the time or opportunity to do what the people on United 93 did. They had the opportunity to gather their wits about them, communicate over the telephone, find out what was happening that day. Then and only then they organized in the back of the plane to do the honorable and brave effort that they made in Shanksville, Pennsylvania.

I would like to point out that the fortified flight deck door provides hijackers with a benefit that the people on United 93 didn't have. The hijackers inside a fortified flight deck would be protected from those who attempt to overrun the airplane. So we still have the same challenges we faced on 9/11; however, at all levels our security has greatly improved from what we had that morning.

Ms. JACKSON LEE. I thank the gentleman.

I am trying to acknowledge or will acknowledge Congresswoman Eleanor Holmes Norton, a member of the committee. And we will yield now 5 minutes to Congresswoman Clarke of Brooklyn, New York.

Ms. CLARKE. Thank you very much, Madam Chair, Ranking Member Lungren.

Madam Chair, I would like to receive unanimous consent to receive the statement of Marcus W. Flagg, president of the Passenger Cargo Security Group and the Federal Flight Deck Officers Association, who unfortunately was unable to be here to testify today.

Ms. JACKSON LEE. Without objection, so ordered.

[The information follows:]

FOR THE RECORD

PREPARED STATEMENT OF MARCUS W. FLAGG, PRESIDENT OF PASSENGER-CARGO SECURITY GROUP, AND THE FEDERAL FLIGHT DECK OFFICERS ASSOCIATION

Chairwomen Jackson-Lee, Congressman Lungren, Members of the Subcommittee:

I am pleased to provide testimony before you this afternoon on the Government Accounting Office report, discussing Federal Coordination for responding to In-flight Security Threats. I am a United States Naval Academy graduate, a former Navy fighter pilot and a graduate of the Naval Post-Graduate School on Aviation Safety. I am also currently an airline pilot with UPS Airlines. On September 11, 2001, my father RADM Bud Flagg USNR and my mother Dee Flagg died aboard American Airlines flight #77, when it was commandeered by terrorists and crashed into the Pentagon.

Since 2001, I have been proactive in improving aviation security to help protect our country against terrorism. I currently serve as president for two aviation security organizations. In 2005, I co-founded the Passenger-Cargo Security Group (PCSG), which is a non-compensated, not-for-profit trade association formed by commercial pilots from passenger and all-cargo airlines. These pilots fly for several different airlines, and are considered experts in aviation security from their work together on various airline security projects. PCSG continues to work with regulators, and members of Congress, and has provided testimony in the past for both the Senate and House.

I also serve the not-for-profit and non-compensated Federal Flight Deck Officers Association (FFDOA) as its president. FFDOA represents Federal Flight Deck Officers (armed pilots), which now represent the third largest Federal Law Enforcement organization in the United States. The FFDO program is an extremely viable, cost effective, and successful element of our national aviation security effort today.

Security Philosophy

PCSG believes in integrated security solutions that work together as a "system of systems" providing the maximum deterrent against terrorist attacks at the lowest possible expense. Flight crews are a key element in an integrated security system and are an asset that has yet to be fully exploited. Aircraft on the ground should be protected with security measures that begin in the cockpit and radiate outward to the airport parking lot and beyond. This clearly requires the cooperation of several different entities. Once a flight is airborne, only on-board assets can affect the positive outcome of a security breach. Therefore, it is crucial that flight crews have the training and information necessary to influence a safe outcome. The lives of hundreds of innocent Americans on-board the aircraft and thousands on the ground hang in the balance. Nothing can be made terrorist-proof, but intelligent and coordinated programs can provide a powerful deterrent to those who might attack the aviation interests of our country.

Cockpit Defense

Federal Flight Deck Officers (FFDOs) are the first line of deterrence and the last line of defense. This is the most cost effective security measure we have to date. FFDOs are trained to stop a threat using the full spectrum of the force continuum. While the training is consistently reported as excellent, serious questions remain about the Transportation Security Administration's (TSA) administration of the program. Including the complete omission of the FFDO program in Secretary Hawley's most recent testimony dated October 16, 2007. The FFDO program is a growing federal officer corps, but many more pilots are needed. Those volunteers will not be forthcoming unless fundamental changes in carriage, liability, time for training without airline obstruction, and international coverage are made to the program.

Officer safety should be "number one" without question, as well as the safety of passengers. No one in law enforcement handles a firearm as many times a day as an operating FFDO per the TSA Standard Operating Procedure (SOP). This is a formula for an accidental discharge. The transporting protocol will lead to the loss of firearm retention, directly contradicting sound law enforcement practices, and the participating FFDOs should be commended for superior performance against a poorly constructed SOP. The politicizing of procedures and defiance of law enforcement lessons-learned places FFDOs and others in the airline environment at risk, as well as poses a liability on many fronts. The FFDOs should use transporting a locked firearm as an option, but otherwise carry their firearm on their person. The September 2001, FBI Cockpit Protection Plan provides a 6-day course to arm 60,000 pilots in two years using full time carry protocol.

A FFDO as a flying pilot would defend the aircraft from the cockpit only, and not exit the cockpit door. If one or more FFDOs are riding as passengers in the back

of that same aircraft, they may be the only law enforcement on board (including cockpit crew). They should not be restrained by the government from defending the cockpit in the event of a terrorist attack regardless of the side of the cockpit door they are seated. The absence of this element of the program is very damaging on more than one front. On September 11th, a Federal Officer was on board United Airlines flight # 93. Unfortunately, due to the FAA and his agency policy, his weapon was located in the belly of that aircraft. Threat assessment aside, the inability to operate internationally translates into many FFDOs who may not operate domestically, since they fly mixed schedules. This specifically takes trained FFDOs out of the system. Currently, FFDOs operate four times the coverage of the Federal Air Marshal Service at 1/25th the cost.

Cabin crewmembers should also be trained in defensive tactics (DT). Airline managements have resisted this valuable training and prefer to view cabin crews as mere food servers.

Proper employment of defensive tactics could provide cockpit crews with critical time to prepare a cockpit defense plan and land the aircraft. Currently, the TSA has developed an outstanding Crew Member Self Defense Training (CMSDT) program that all crewmembers may take as often as they like. TSA should mandate the airlines to provide CMSDT to crewmembers, and enable each airline to teach this course at their crew domiciles. As a volunteer program that requires crewmembers to pay for their own travel and hotel expenses on their own time, mitigates the value of this excellent course.

The cabin crew should also have a remote means of communicating with the cockpit crew in the event of a security breach, in addition to their present antiquated primary and secondary communication methods. The Airline Transportation Association (ATA) lobbying efforts defeated legislation mandating such a system. The ATA also lobbied against cameras in the cabin of passenger airliners, a method to help provide the cockpit crew with vital information. These systems cost less than the entertainment systems that many airlines have installed.

The Federal Air Marshal (FAM) program, although another excellent layer of security, has serious shortcomings, not the least of which is an agency of insufficient size. The Federal Air Marshal Service also manages the current FFDO program. An improvement to this viable program would be more involvement and cooperation in training with FAMS and FFDOs. This would require additional funding to support and train the FAMS/FFDO team concept. Presently, FAM Field Offices cannot accommodate FFDOs who wish to use the FAM facilities to improve their skills and teamwork.

Of all the proposed aviation security enhancements available today, "flight deck secondary barriers" represent the single most effective additional layer to protect the flight deck from another potential hijacking. Congress mandated the installation of flight deck hardened doors in 2001, but at the time didn't anticipate the need for a secondary barrier. PCSG and almost every other industry group have since come to the conclusion that a hardened door alone does not provide a predictably reliable barrier to an attack. In order to effectively protect the flight deck during times that the door is opened in flight, the crew needs a protected space behind the flight deck door, and a few seconds to respond to an attempted breech.

Secondary Barriers, such as those currently installed on some of United Airlines airplanes, provides crews the essential space and time to accomplish a door transition. Secondary barriers are extremely inexpensive when compared to other security systems, can easily be installed, and can be easily incorporated into current flight deck access procedures as currently modeled by United Airlines and other carriers. Most importantly, like the mandated hardened flight deck doors, a Congressional mandate of secondary barriers would result in a significant layer of aircraft security in minimal time. In order to expedite this security enhancement Congress should fund the cost of installing secondary barriers, including reimbursement of carriers who are already beginning to install this much needed aviation security enhancement.

A major problem for all three layers of security is that there is no integration of training, or at the least, a clear understanding among each group on how to work together. These three systems have been "stove piped." In addition, the TSA does not require crewmembers to receive operational Security Directives or Information Circulars. The TSA provides this information to airline corporations and lets them decide who the "need to know" employees are. Very few airlines have chosen to share this vital information with cockpit and/or cabin crews. A notable example of the failure to disseminate information to airline crews was the Richard Reid "shoe bomber" incident. Previously, crewmembers were not told of an existing threat to passengers involving explosives in shoes. It was not until after this event that American Airlines elected to change their policy. Other airlines provide only a mini-

mal and cryptically scrubbed version, usually in an untimely manner. It is unconscionable that the TSA leaves this crucial information to individual airline policy or negotiations, and does not require delivery of the operational information to pilots and cabin crews.

Cargo Security

Dramatic growth and maturity for the all-cargo airline has occurred over the past 30 years. In their earlier days these airlines were not very big, and operated at night beyond the view and consciousness of the general public. Today, they are large global airlines that operate around the clock, flying the same aircraft in the same flight environment as the passenger carriers do.

For years all-cargo airlines were exempt from many of the government safety and security regulations required of passenger carriers. One such example involves a critical airborne Traffic Collision Avoidance System (TCAS) that was required of passenger aircraft, but not mandated on cargo aircraft until 13 years later. This lack of uniform safety standards continues today as illustrated by their being no requirement for airport Aircraft Rescue and Fire Fighting (ARFF) to be provided for the all-cargo aircraft, nor for the first responders to conduct any training on all-cargo aircraft. Hardened cockpit doors are non-existent on cargo aircraft, although mandatory on passenger aircraft. The TSA has stated that all-cargo aircraft have the highest risk for hostile takeover. Hardened cockpit doors should be mandatory on all current and future all-cargo aircraft. All-Cargo carriers routinely receive exemptions from government regulations imposed on passenger carriers. Unfortunately, this same double standard is placing all Americans at risk.

A new Full All-Cargo Aircraft Operator Standard Security Program (FACAOSSP) does mandate security training to crewmembers of all-cargo airlines. However, the original requirement was reduced at behest of the Cargo Airline Association (CAA) and ATA by fifty percent and is clearly insufficient in regards to training initial crewmembers. Many all-cargo airline corporations have fought against the training for their pilots claiming the cost is too great. When pilots have petitioned their companies to work with them to develop programs, airline managers have told them they would refuse to incorporate such training unless it is regulated by the government. It would seem obvious that an all-cargo B–767 can cause just as much damage as a passenger B–767, whether hijacked or detonated over a populated area. This is a fact that has been lost on airline managements with an economic bias, keeping them rooted in the old ways of doing business, hoping nothing will happen again, and believing they are not responsible for security.

There has been no positive response as to when the All-Cargo Common Strategy will be accessible to the crewmembers. This working group ended almost two years ago.

Government regulation and planned programs fall short of what is required to shore up this weakness in our aviation security. Unfortunately, our government and airline managers are ignoring the fact that China and two major European cities have been using electronic inspection equipment successfully for the last five years. These foreign airports have demonstrated dramatic statistics of reduced contraband, smuggling, and terrorist related shipments. These tools would enable the United States to be proactive, versus doing little to nothing, and are not cost prohibitive either in acquisition or in throughput.

Airport security standards have seen minimal enhancement for the all-cargo operation. While minor improvements are underway for larger airports, many smaller airports are not required to have an airport security program, and are still not required to make any changes even though they host large jets and are located near major populated areas. Once again the excuse given is the fear of "financially overburdening" the all-cargo airlines. Additionally, the TSA does not want to establish new rules that may be difficult to understand by people that never had to follow them at unregulated airports.

PCSG believes in "one level" of security for cargo on passenger and all-cargo aircraft.

Crew Screening

Physical screening of crewmembers prior to flight is conducted as part of the TSA program for providing airport and flight security. Designed to prevent another 9/11-type attack, this method of screening crewmembers can never prevent such a disaster. Legitimate crewmembers must obviously have access to aircraft in order to fly them, and therefore do not require a screening routine designed to stop potential terrorists at the passenger screening portal. Therefore, for crewmember screening to be meaningful, the process must be able to confirm or deny the identity of an individual as a crewmember so as to prevent unauthorized access.

PCSG calls on the TSA to conduct this security function in a manner that will truly protect the civilian population. Crewmembers are the most vetted employees in the civil aviation system with countless checks on their abilities and backgrounds. Pilots have their hands on the controls of what is now considered a potential weapon of mass destruction, so in effect, physical screening is meaningless. Crewmember screening must simply address the issue of confirming access authority. There are several off-the-shelf systems available that are capable of such a task, including biometric solutions and database solutions already approved by the TSA and FAA. In addition to Cockpit Access Security System and Department of Justice INS FASTPASS, countless other crewmember screening systems have been proposed to the TSA. Current practices which screen crewmembers in the same manner as passengers waste valuable resources that could be put to better use elsewhere. The TSA currently screens more than 2,000,000 pilots monthly.

Two years ago, on May 13, 2005, I provided testimony to this committee on Aircrew Screening. The TSA once again promised the Transportation Workers Identification Card (TWIC) would be the solution to all credentialing. This program has had marginal success and is proof positive, that one size does not fit all, especially when it comes to aviation. Canada has implemented a workable biometric ID program. Even Walt Disney World has biometrics for its season pass holders. If the Mouse can do biometrics, surely the Government can also.

A National Law Enforcement Biometric Identification Credential was produced to confirm positive LEO status anywhere in the country. This program could be piggybacked for airline pilots instead of waiting on the TWIC program.

Passenger Screening

PCSG recognizes the nature of a changing threat, and the necessity for a proactive approach to mitigate that threat. There are solutions for passenger screening that rely on physical security, technology, and the human element. PCSG believes that the TSA has made large investments in time and money building a system that looks for dangerous "things" instead of dangerous people. We are convinced that this approach is fundamentally flawed.

The current state of passenger screening in the United States has made some limited improvements over the screening methods from pre-9/11. More "process" has been added in an effort to create a serious, but not necessarily more meaningful, screening environment. The selectee process is significantly flawed and the secondary screening provides little if any advantage over the initial primary screening.

One of the most serious drawbacks to the present system is that the TSA has been pushed and pulled in different directions by many competing interests. The airlines continue to use (and have sole authority over) the subjective CAPPS I (Computer Assisted Passenger Pre-screening) system for "profiling." Unfortunately, the airlines scrubbed everything useful from the original CAPPS I program out of fear of discrimination law suits. In an effort to make it without bias, they have made it ineffective. The criterion to become a selectee has little bearing on potential terrorist activity, and with a significant percentage of passengers selected it has more of a harassment effect than to serve as a true security feature.

The TSA has attempted to take control of the CAPPS program with a second-generation format. This program was hailed as having the ability to fix many of the problems that presently exist and to be operated by the government, instead of each individual airline. At present CAPPS II is mired down with serious problems and the TSA has no solution in sight.

There is a system that exists that would provide a dramatic improvement in anti-terrorism mitigation, and provide an additional bonus of customer satisfaction. It is known as Behavior Pattern Recognition (BPR). The TSA currently uses a trimmed-down version of BPR called Screening Passengers by Observation Techniques (SPOT). The SPOT program only teaches TSA Security Officers how to detect one of three main elements that make BPR work. The other two elements are delegated to the airport law enforcement officers, who clearly are the backbone of airport security. As trained law enforcement officers, they have the bearing, temperament, and most importantly, the authority of law to conduct this important security feature, although they are not presently required to receive BPR training. If the full BPR were to be used by TSA Security Officers as a major screening method, experts report that selectee counts would be reduced from the current high numbers, down to a very low percentage. Additionally, that significantly smaller number would receive a more thorough and meaningful secondary screening than presently exists. This serious, behavior-focused program is specifically designed to look for traits exhibited by those with threatening intent.

Pilots, flight attendants, and certain airline employees are excellent candidates to receive training in the SPOT or BPR program since the majority of their time is

spent throughout the airport environment. Once again, this is an untapped potential that TSA will not address.

At the passenger screening portals, the ability to keep threatening intentions and material, such as explosives, off the aircraft cannot depend on the current x-ray machines and TSA screeners alone. Chasing every tool a terrorist may use is sadly ineffective.

As we look at technology, we recognize it has a necessary and evolving role in the passenger screening effort. A properly-run BPR program in combination with K–9's, or their technological equivalent (such as fluorescent polymer), can be very effective at mitigating many types of "carry on explosives" and other threat behavior; "looking for bombers, not for bombs". Magnetometers, or metal detectors, have been staples of passenger screening for decades. Both walk-through portals and hand wands continue to be useful tools, but portals are becoming enhanced to be trace explosive detectors also. Some airports are installing such devices, commonly called ″puffers″, since they blast a puff of air as a passenger passes through in order to collect and test for explosive elements. The use of x-ray technology can be added to these portals, but many passengers have privacy concerns over the display of their body images. These images can be ″cartooned″ so actual body types are not displayed.

Screening devices for carry-on bags have enhanced features (that have been in place for many years), but the government is preparing to further enhance these units with existing bomb detection technology. Detectors are in development for liquid explosives, but they are presently too slow and lack sufficient accuracy. Bomb sniffing dogs (K–9s) have their limitations, but are very accurate, and also serve as an outstanding interim fix while we wait for future technologies currently in development. Closed Circuit Television (CCTV) is a good tool for tracking and documenting activity in the entire airport environment, from the parking lot to the airplane.

Physical security is being adjusted at many airports. This will be an essential design feature for future airport projects. Parking lot locations, terminal stand-off features and materials, as well as electronic "one way" gates to help prevent portal breaches, will be among the approaches to this important element affecting passenger screening.

MANPADS

Man Portable Air Defense System (MANPADS), otherwise known as shoulder-fired missiles, pose a clear threat to commercial aviation. Over the past twenty years, numerous aircraft have been fired upon by MANPADS in countries outside the U.S. The proliferation of MANPADS has escalated to the point that there is now serious concern of an attack in the United States.

Economic realities may prevent retrofitting the entire U.S. airline fleet with the most expensive MANPAD countermeasures. Of primary concern is the Civil Reserve Airline Fleet (CRAF). These large jets are U.S. registered airliners (both passenger airlines and all-cargo airlines) that fly in support of our U.S. troops abroad. At present they are the most vulnerable, and should be outfitted first. Also, different manufacturers provide different successful solutions. MANPADS is not an airport perimeter issue. The operating envelope of this weapon system could enable an attacker to be "away" from the airport environment.

TSA

It has been over six years since September 11th. The TSA was formed to standardize aviation security. This is not the case. Each airport is its' own domain, isolated in its' exclusive security plan. Consistency throughout the system is non-existent. Every year, the TSA testifies about airport access and employee problems, but does little to address this serious problem. Past TSA congressional testimony always claim credit for working towards solutions, but is shallow on achievement. Why? Because the TSA has ceded its' authority to allow the airport security directors to run the show. Additionally, the TSA has become an inflexible bureaucracy, resistant to new ideas from stakeholders. Meetings and working groups are used to reinforce their existing policies and to placate the GAO reports. TSA is a reactive regulatory agency unwilling to provide proactive changes. TSA officials, for the most part, do not have an aviation background nor do they understand the industry they are attempting to protect.

Summary

Aviation continues to be the favorite target of terrorists. This threat is real and evolving therefore we must stay one step ahead of the terrorists. Any attack on aviation would ground the nation's airline fleets with a resulting economic impact estimated by the Department of Transportation to be $10 billion U.S. dollars per

week. This figure, of course, does not account for the potential tragic loss of human life in the air and on the ground.

Pilots and cabin crews are active participants in aviation security and will live and die by TSA decisions and policies. Every day, pilots and cabin crews operate in an environment with no margin for error. Since man began flying, aviation has been inherently dangerous, and today's airline pilots know that the FAA rules and regulations are all written in blood.

Many resources from various elements of security must work together to best mitigate a terrorist threat. In the event of terrorist action, once airborne, the only viable resources are on the aircraft.

Madam Chairwoman, and members of the Subcommittee, I thank you again for the opportunity to provide testimony today. I am happy to respond to any questions which the subcommittee may have.

Ms. CLARKE. Thank you, Madam Chair.

I would like to direct my first question to Mr.Gage. From your testimony it appears that the transportation security officers have many issues with regard to how they have been treated by TSA. Generally speaking, what impact do you believe this has had on morale, and has this treatment led to a high level of turnover in the ranks?

Mr. GAGE. I have to believe it does. Of all the government, Homeland Security has the worst rating for morale in the government. And in Homeland Security the TSOs have the worst morale. So this is the worst of the worst that we are talking about. And clearly, as I said, it is a choice TSA management makes. They don't have to deal with folks like this. They don't need this repressive system. They don't need almost a militaristic type of view for simple sicknesses or child care leave or those type things that I think build a professional workforce and one that has good morale. And I think good morale is crucial in this job. I think teamwork and morale is absolutely crucial.

Ms. CLARKE. Thank you, Mr. Gage.

Ms. Friend, in your testimony you discuss the need for coordination between flight attendants, pilots and air marshals. What type of coordination do you envision and do you believe is the responsibility of the airlines and the DHS to facilitate this?

Ms. FRIEND. Each of us has training, and we know what our reaction would be to any emergency situation, but we don't train together, so we are not always assured of knowing what the other group—how they are going to react, and that is a situation that can have really disastrous results.

If I may, I will just give you one brief example of it that happened fairly recently on a flight. The aircraft, as they were taxiing out, one of the flight attendants identified an object that had all of the components or appeared to have all the components of a bomb. The flight attendant reacted appropriately. There was a Federal air marshal on the flight; notified the cockpit, notified the Federal air marshal. The flight deck pulled the aircraft off to the side, made an announcement to the passengers without unduly alarming them that there was a situation they needed to check into, and then announced that while we were waiting here, it would be okay to use your cell phone.

The Federal air marshal reacted immediately, jumping to his feet, pulling his weapon, saying no one can use your cell phone, because the Federal air marshal was fearful that someone would use a cell phone to detonate this device.

It is a situation that could have been prevented with better communication and better training for the groups together.

Ms. CLARKE. And then my follow-up to that is do you believe that it is the responsibility of the airlines and DHS to facilitate this? Who would you see as the entity that would ensure that this happens? Because clearly what you have described is something that anyone would envision if such integral partners are being trained in isolation of each other.

Ms. FRIEND. Well, it would require the cooperation of DHS and/or the TSA, because the Federal air marshals are not under the direct supervision of the airlines. So it would require a coordinated effort.

It would also require an economic investment, which has been the problem, is that there is a reluctance to make that economic investment in better and more comprehensive training, at least for the work group that I represent.

Ms. CLARKE. Thank you very much.

I would like to ask also, would there be any benefit in further coordinating with the TSOs since all of you share the same goal of protecting the public as they travel through the skies? Have you given any thought to that, Ms. Friend?

Ms. FRIEND. I'm sorry, would you ask me that again?

Ms. CLARKE. There is one group that we all acknowledge is part of the continuum of safety in our airports, and that is the transportation security officers who oftentimes are near the frontline, right?

Ms. FRIEND. Right.

Ms. CLARKE. Would you see any benefit to them also coordinating with the others in terms of protecting passengers and crews and all of that?

Ms. FRIEND. Well, it is always helpful for every layer of the security system to understand what the role is of the other layer. But we do not have—I mean, the direct contact we have with the TSOs is during our process through the security checkpoint during which we are really not much different from the average passenger clearing security. And I am not aware that we really have any significant issues with the TSOs. I think we have a very amicable relationship, as far as I know.

Ms. CLARKE. Thank you very much, Madam Chair.

Ms. JACKSON LEE. I thank the gentlelady.

Now it is my pleasure to yield 5 minutes to the distinguished gentlelady from the District of Columbia, Ms. Eleanor Holmes Norton.

Ms. NORTON. I want to thank the Chair. And I particularly thank you for this hearing. I am on the Aviation Subcommittee, and I find this hearing of value.

Some of the issues recur. Let me ask Mr. Gage in particular about a statement that appears on page 3 of his testimony about the TSOs' high attrition rate. You describe it as incredibly high. I think that is not an overstatement; in the first 8 months of 2007, an attrition rate of 19.6 percent, much higher than the current 2.2 percent attrition rate of the Federal workforce. This kind of instability is associated with low-level jobs, not security jobs. And I would be interested in why you think there is this incredibly high turnover rate, which I take it is people leaving or resigning.

Mr. GAGE. Voluntary as well as involuntary. I mean, there are quite a few people that get fired there, too.

Ms. NORTON. Why do they get fired?

Mr. GAGE. What?

Ms. NORTON. Fired for a cause?

Mr. GAGE. Well, some of the reasons are pretty weak, and there have been quite a few cases that are being turned over. But I think the whole—the pressure of the job, the structure of the job itself, which has been flexible, the fact that the staffing levels are so low, which really puts additional pressures on the workers in regards to taking leave, with regards to getting their training, just the general pressure, the overall pressure of the job. This staffing problem is going to have to be addressed, because it causes an additional staffing problem with people additional people leaving.

So fully staffing the TSOs I think would go a long way and, also, I think just treating people more professionally would go a long way to—most of these people have had other careers, professional careers. Some are teachers, and they are just not used to being treated in the way that they are without having any say, afraid to make any type of suggestion or comment for fear of reprisal.

So I think there is a whole general attitude there that needs to be cleaned out, and some of the choices that TSA has made on how to run this important piece of business just has to be re-evaluated and modernized.

Ms. NORTON. Well, you indicated somewhere in this testimony, as I recall it, that when a TSA employee reports an issue, a security issue, that—oh, here it is. It is on page 6.

Much of your testimony, it is just inconsistent with what we have to demand as that of security. The high turnover, something has got to be done about that. That is why so much training, as you report in your testimony, has to go with new people, just to keep the new people going so you can't train the people who are already there. That is not what we expected when this was transferred to the Federal Government. It has been inconsistent with the way in which other Federal employees respond and are treated.

You say, though—and this really caught my eye—TSA refuses to be bound by the Office of Special Counsel recommendations when TSOs are retaliated against for blowing the whistle on security breaches. I need to know more about that because, obviously, that could conceivably concern security.

Mr. GAGE. TSA is not bound by virtually any of the safeguard-type of provisions.

Ms. NORTON. Having whistleblower protection?

Mr. GAGE. That is right.

Ms. NORTON. There is no whistleblower protection?

Mr. GAGE. There isn't.

Ms. NORTON. Madam Chair, there are two points right there. One, turnover, as long as you have got something, these people going in and out, I don't know how we can consider that this is a workforce for security. And if you cannot blow the whistle when you see something—of course, they don't have any union in the first place—without fear of losing your job, I guess the best thing to do is just let it go by. Very disturbing.

Ms. JACKSON LEE. We are not ending your time. I am dismayed to indicate that we need to clear the room. There is a package unidentified, unless someone in this room can identify it. So we have to clear the room, suspend the hearing for just a moment and ask all individuals, as I have been instructed by the Clerk, to clear the room just for a moment.

[Recess.]

Ms. JACKSON LEE. Let me ask for a zero on the clock. Thank you.

To the witnesses, if there is ever anything that you get here in Washington, in a complete opposite of what people perceive as real-life experience, and so you are in the Homeland Security Committee, and you just had real-life experience. We are glad, however, that it resulted in a false status. So thank you very much.

I am going to proceed with my line of questioning, and I will yield myself 5 minutes as we conclude this hearing.

Congresswoman Eleanor Holmes Norton was really tracking a line of questions, Mr. Gage, that I think are enormously crucial. And before I do that, let me ask unanimous consent to submit into the record the Federal Law Enforcement Officers Association, and I can do this because a quorum has been established. Hearing no objection, it has been submitted into the record.

Ms. JACKSON LEE. This recounts for us one sentence: "A recent news report showed that 75 percent of fake bombs or bomb parts got past TSA screeners at Los Angeles International Airport and 60 percent got past TSA screeners in Chicago O'Hare."

Even though this data may have been in place for a period of time, I think it speaks to Mr. Gage in terms of his points regarding training and also technology.

So I want to go to Mr. Gage again to ask, what are the issues—as I survey our TSA screeners, one, I want to thank them for their service for fear of them thinking that that is not our intent here today. But I do notice or do get an opportunity to hear of long hours, of painful working conditions, some airports don't have rest areas, and those are basics, but they all contribute to the way one does one's job.

But the other question, Mr. Gage, is professional development. The ability—I asked the question of TSA itself. What is a route—what is the professional route for a TSA screener? That always gives one the ability to stick in there.

I cite the huge hours, though a different circumstance, of interns—of medical interns, residents who work unbelievable hours, hours not seen in any other professional capacity. But, in any event, they stay the course because they are going to be a doctor. So that seems to be a concern. Will you share with me your thoughts about that?

Mr. GAGE. Yeah. I think the avenues of promotion are very limited. I guess you could possibly become a trainer or a supervisor, and I think that is about it, which is—and for the vast majority of the workforce, there simply isn't any profession promotional potential, and I think that is going to really force this into an almost part-time workforce, which I think would be a disaster.

Right now, there is 20 percent or so that are part time. And as full—time people or people looking for a career, certainly the money is not there and the promotional opportunity is not there,

and I think that is just going to require or force airports to be hiring part-time people, and I think that just exacerbates the whole problem.

Ms. JACKSON LEE. Thank you.

Let me see if I can explore this question that I had for Ms. Friend. Tell us again—I think it is really crucial, and we expect to have the air marshals before this committee and air traffic control. That is different. But I think it is important not to highlight some unfortunate circumstance, but coordination is key. And an airplane is like a closet. There is nowhere to go. And maybe even worse because, obviously, a closet might have a door. But say a locked closet. There is nowhere to go.

And the answer that you presented was stark, which is a flight attendant giving basic instructions from his or her experience and a law enforcement contravening it but then creating what I think might be a scene of tension or confusion for the passenger.

Speak to this coordination question again, particularly flight attendants who really are the people movers. They are moving about. They are also looking at behavior of passengers. Speak about coordination and the importance of training flight attends.

Ms. FRIEND. Well, I mean it is critical that each of us who play a role in onboard aviation security have a complete and thorough understanding and expectation of what the other two parties' role is. I mean, I think that is just plain common sense that I know what the Federal air marshals' expectations are, what their instructions are in certain circumstances and that the air marshals know what mine are and that the flight crew know what to expect from each of the other two pieces in the cabin. Otherwise, we end up getting in each other's way and not accomplishing anything, I mean, and not accomplishing our goal, which is to protect the travelling public.

If I have to stop or if the air marshal has to stop or if the captain of the aircraft has to stop and say, okay, what are you going to do now, then we lose valuable time. We need to each understand what each other's role is and get out of each other's way, to be frank with you, and let each of us do our job.

Ms. JACKSON LEE. Wireless communication, a lot of people would raise the question. Of course, they would raise the question, what would be the revenue source for that as we look at the legislation, write the legislation? We know we will craft a revenue stream, and we would hope for the cooperation of the airlines, since we——

I remember very distinctly cooperating after that tragic 9/11 event, recognizing the financial hit they had taken. This Congress rose, if you will, to answer the call. And wireless communication, to me, eliminates the sitting duck status of a flight attendant using this heavy equipment at the front and maybe at the back while everyone is watching and certainly those who would be interested in doing harm. Why don't you share how you see the wireless being helpful?

Ms. FRIEND. Right. I mean, I can give you an example of that. In a simulated terrorist attack, the first thing that those individuals acting as the terrorists did was cut the wire on the interphone so that the flight attendants could not communicate with the cockpit. That is just logical. But as far as the venue stream or funding

mechanism, I really believe that the airlines themselves should be responsible for providing that as a piece of safety and security equipment onboard the aircraft, just as they are required to provide fire extinguishers and first aid kits and external defibrillators.

I think the problem here is that the airlines themselves, the people who manage or mismanage this industry, do not—they look at security concerns as sort of extraneous to the service that they provide. When, in fact, ensuring that the people that they are selling tickets to and promising to transport safely, that is a part of the service that they have contracted to provide to the travelling public. And so I think that they should be fully responsible for that piece of safety equipment, just as they are other pieces of safety equipment.

Ms. JACKSON LEE. Very instructive. Let me finish.

Captain Hesselbein, one of the things that struck me was the leave time to, in fact, comply with requirements for your pilots to comply with a law that was passed by this Congress. What has been the problem with just doing this through personnel, through a personnel structure that if you have a specific training that could be used for your job that you have that time to be trained or to be retrained? What is the problem that you are finding?

Mr. HESSELBEIN. The problem is that many employers find their pilots resource is scarce at the present time. There are also those who do not believe that there is a role for an armed pilot in the flight deck. Those two, combined with the fact that there is no law in place that allows them to take leave, causes the problem.

I spent many, many years in the Air National Guard; and during my time there before I retired, it was a very good thing to be able to walk in to my employer with a set of orders saying, I have to leave my place of employment for 60 days to deploy to one place or another, and the employer had to permit me to leave my employment to serve my country and then return to my job.

FFDOs are serving their country when they go to train to protect their flight decks. They should have that same right.

Ms. JACKSON LEE. I think this has been enormously instructive; and let me just add, in conclusion, just to recite from a letter that I offered into the record from Mr. Chris Paris, again, focussing on air traffic control. And it really adds to the testimony that has been given here today. It really speaks to missing elements that each of your constituents have that keeps them from performing at an excellent rate their jobs and that impacts on American security.

It relates to this story coming from Houston. There is a bar by the FAA from having utilization of defibrillators in the air traffic control unit. Now I would not suggest that everyone is under tension, enormous tension. But I imagine that there would be a few air traffic controllers who do their job very well but would tell you that it is very seriously, a very serious, if you will, tension-filled responsibility. I think when I visited with some of them, they indicated they are to be on a certain number of hours and off just because of that. So the FAA bars defibrillators from being in the center.

And, unfortunately and tragically, a tribute to this gentleman whose name has been printed here, John Sanfelippo had a heart attack as an air traffic controller, no defibrillator, and tragically 14

minutes before attention could come to him. And, of course, tragically he lost his life. I put his name into the record simply because it has been given to me.

But this hearing was to find out what you needed and how this committee could respond to your needs. It is also to thank you on behalf of our ranking member and the members of our committee and just to indicate that a number of members had overlapping responsibilities, and I thank the members for their presence here today. So my gratitude for the witnesses for their valuable testimony and the members for their questions.

The members of the subcommittee may have additional questions for the witnesses, and we will ask you to respond expeditiously in writing to those questions as they are submitted.

And I would, again, emphasize that the partnership of security in America has to be with people and tools, people and travel modes, people and equipment; and your presence here today reinforces that.

I thank you for your testimony. We look forward to working with you and curing some of these problems.

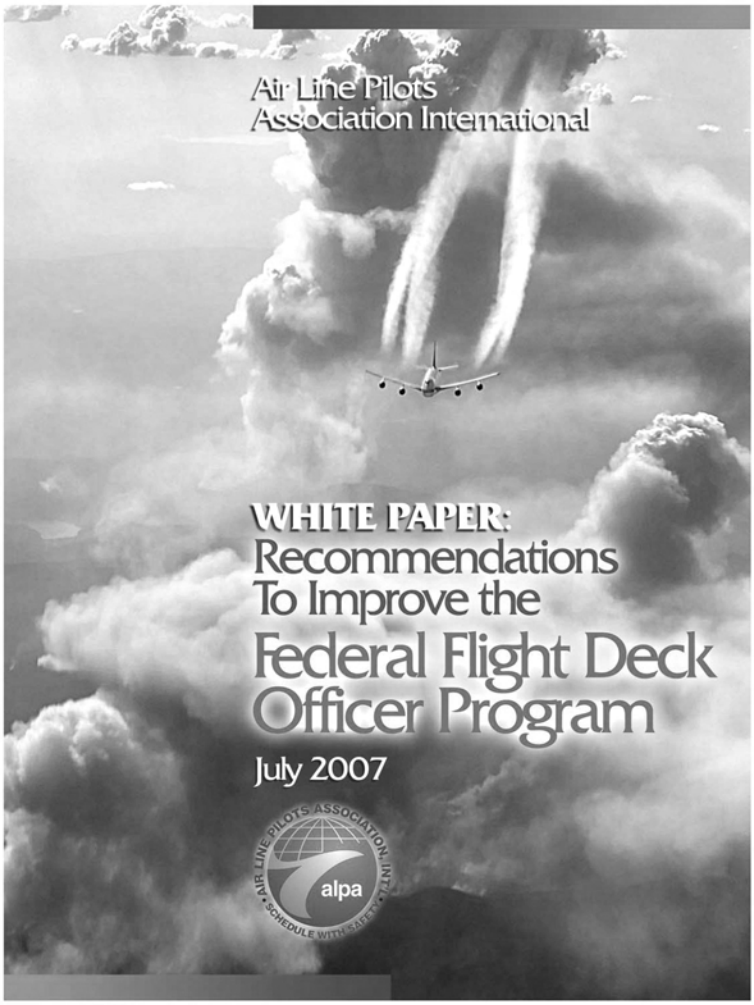
With that, hearing no further business, the subcommittee stands adjourned.

[Whereupon, at 4:25 p.m., the subcommittee was adjourned.]

VerDate Nov 24 2008 07:10 Sep 04, 2009 Jkt 000000 PO 00000 Frm 00106 Fmt 6601 Sfmt 6601 H:\DOCS\110-HRGS\110-77\48972.TXT HSEC PsN: DIANE

Appendix: Attachments

Attachment A



ALPA WHITE PAPER

AIR LINE PILOTS ASSOCIATION, INTERNATIONAL
1625 Massachusetts Avenue, N.W., Washington, D.C. 20036
703-481-4440 • MEDIA@ALPA.ORG • WWW.ALPA.ORG

Recommendations to Improve the Federal Flight Deck Officer Program

ALPA was the first organization to call for the creation of the Federal Flight Deck Officer (FFDO) program, which became a reality when the Arming Pilots Against Terrorism Act (APATA) was enacted as part of the Homeland Security Act of 2002.

The Air Line Pilots Association, International (ALPA), founded in 1931, represents the safety and security interests of 60,000 pilots who fly for 41 U.S. and Canadian domestic and international passenger and all-cargo airlines. Based on our considerable experience and vested interest in airline safety and security, we offer our views regarding the Federal Flight Deck Officer program. To learn more about ALPA, visit the Association's website, www.alpa.org.

Executive Summary

To ensure the Federal Flight Deck Officer (FFDO) program's continued viability, several of its key components need to be improved, particularly in the areas of transporting and carrying weapons in domestic and international airline operations, jurisdictional authority, pilots' leave and personal expenses for training, communications and support of field-deployed FFDOs, and requalification and recurrent training.

ALPA is committed to continuing to provide its expertise to the Transportation Security Administration (TSA), the Federal Air Marshal Service (FAMS), and Congress to ensure the safest, most prudent, and most efficient implementation of the FFDO program.

While several of the 12 specific areas in which ALPA believes the FFDO program needs improvement can be resolved by the airline industry and other stakeholders (including ALPA), others may require congressional involvement (see BOX, page 2).

A solid program

ALPA was the first organization to call for creation of the Federal Flight Deck Officer (FFDO) program, which became a reality when the Arming Pilots Against Terrorism Act (APATA) was enacted as part of the Homeland Security Act of 2002.

The first class of 44 federal flight deck officers graduated from training in April 2003. Since then, thousands of airline pilots have been trained and deputized as FFDOs. Because the majority of these federal law enforcement officers are ALPA members, the Association has a vested interest in the integrity and viability of the program and remains engaged in a close working relationship with the TSA and the FAMS to ensure the program's continued success.

Because of initial government and industry uncertainties about how effective and reliable the program would be, it was deployed in an extremely cautious manner, at times in conflict with recommendations made by aviation security and law enforcement experts. Examples of this restrictive approach can be found in the initial weapons transport and carriage protocols, the language of the original credentials and the decision not to issue a metallic badge to FFDOs.

As we note the passing of the program's four-year anniversary, its reliability,

ALPA White Paper

Federal Flight Deck Officer Program

ALPA recommends that Congress legislate to enhance the FFDO program and include these priorities:

- Improve procedures for transporting and carrying the assigned FFDO weapon to, from, and within the aviation environment to ensure security of the weapon, maximize safety margins, and accomplish the FFDO mission.
- Clarify congressional intent with respect to the FFDO mission to protect the flight deck, particularly with respect to FFDO presence in the cabin of passenger airliners while deadheading, commuting, or traveling for FFDO training.
- Clarify FFDO personal/professional liability issues and protections.
- Ensure FFDO leave for training, similar to military leave, to facilitate and maximize pilot participation.
- Improve field support and management of FFDOs, to include dissemination of intelligence and peer-to-peer communications.
- Define the FFDO internal affairs/disciplinary process.
- Ensure that FFDOs are reimbursed for costs associated with training, including travel, lodging, and per diem.

The Association is committed to continuing to provide its expertise to the TSA, the FAMS, and the U.S. Congress to ensure the safest, most prudent, and most efficient implementation of the FFDO program.

as well as that of the pilots who compose its ranks, has been clearly demonstrated. Initial skepticism has given way to praise and recognition. Federal law enforcement trainers consistently laud the abilities and the attitudes of the pilot volunteers. The TSA often cites the FFDO program as a key component in the layered approach to aviation security. Through it, the United States has gained great benefit from the dedication of airline pilots who are willing to make significant personal sacrifices to provide security for a critical component of the nation's infrastructure.

ALPA appreciates the TSA's significant efforts to develop and deploy the FFDO program and the contributions of the FAMS in maintaining it. ALPA applauds Congress for its vision in recognizing the need for, and the benefits of, the program and for passing the legislation that mandated its creation. The Association is grateful for the opportunity to have worked hand-in-hand with congressional leaders on this most important initiative and is prepared to do so again to advocate for and consult on needed legislative improvements to the program.

From the outset, ALPA emphasized that the FFDO program must be an initiative that selects, trains, and deputizes qualified candidates chosen from the airline pilot population. Dedication to these objectives was critical to success in obtaining congressional approval. Furthermore, increasing the number of FFDOs, while significant for the program's effectiveness, is not the only objective. The quality of the candidate-selection process, basic and recurrent training curricula, equipment, management, and operating procedures are also key ingredients of a successful program.

Because ALPA is convinced that the FFDO program provides significant deterrence against future hijacking attempts, the Association will continue to advocate for improvements and strongly oppose any effort to undo the program's success.

Following are our specific recommendations on ways in which the FFDO program should be improved:

ALPA WHITE PAPER
AIR LINE PILOTS ASSOCIATION, INTERNATIONAL

Federal Flight Deck Officer Program

Transporting and Carrying Weapons

ALPA believes that the U.S. Congress should mandate that within 90 days after passing enabling legislation, the TSA must develop and begin phased deployment of an FFDO weapons carriage program that incorporates a protocol for personal carriage while in transit to, from or within the aviation domain.

Current FFDO standard operating procedures (SOPs) governing the transport and carriage of weapons create the potential for significant safety and security risks within the aviation environment. Evidence of this fact can be found in statistical data collected and maintained by the TSA regarding events involving mishandled and misplaced weapons.

During the course of the TSA-industry stakeholder meetings held in January and February 2003, federal law enforcement experts recommended that FFDOs be authorized to carry their assigned weapons on their person while traveling to, from, or within the aviation domain. Statistical information supporting this recommendation, generated from Uniform Crime Reports (UCR) and an FBI internal study, was presented to the TSA. The data demonstrated that in most cases when a law enforcement officer's weapon was lost, mishandled, or stolen, it had been stored in a container and not carried on the body of the person responsible for its custody, safety, and security.

Despite the recommendations made by law enforcement experts in 2003, the TSA elected to require FFDOs to use lock boxes to transport FFDO weapons. ALPA applauds the TSA and the FAMS for having recently discontinued this protocol. However, the current transportation procedure does not improve the security of the weapon and introduces other unique safety concerns.

ALPA concurs with law enforcement and aviation security experts who recommend that FFDOs not be separated from their weapons while in transit. We consider it vital that FFDOs be further trained and authorized to carry their weapons on their person when in the aviation domain, to include when seated in the cabin of an airliner while deadheading, commuting, or on official FFDO travel. Any additional training must be developed in a fashion that accounts for the realities of pilot scheduling needs.

ALPA understands the narrowly defined mission of the FFDO. We offer these recommendations for two primary reasons: (1) to ensure the safety of service weapons and (2) to make the most prudent use of the FFDO asset as an additional layer of security. ALPA believes that Congress should mandate that within 90 days after passing enabling legislation, the TSA must develop and begin phased deployment of an FFDO weapons-carriage program that incorporates a protocol for personal carriage while in transit to, from, or within the aviation domain.

Mission clarification

SOPs must be rewritten to authorize these protocols and to clearly define the legal rights, duties, and protections afforded to FFDOs in following them.

Recent recurrent-training events clearly demonstrated that circumstances exist in which FFDOs traveling in an airliner cabin would be expected to take enforcement actions that would violate current FFDO SOPs governing use of their weapons. The potential for this shines a spotlight on such issues as FFDO mission, jurisdiction, training, and liability protections that need to be clarified.

Because the primary mission of a flight crew is safe operation of the aircraft, ALPA agrees that no FFDO traveling on the flight deck of a passenger airliner should leave its confines to respond to a disturbance in the cabin. However, ALPA does not support the practice of prohibiting FFDOs who are deadheading, commuting, or on official travel from carrying their assigned weapons in the cabin of an airliner, or from acting to protect the flight deck against acts of terrorism under any circumstances.

ALPA recommends that Congress authorize FFDOs to carry their service weapon in airliner cabins, mandate appropriate training for this change that allows for pilot scheduling needs, and provide for the requisite accompanying liability protections. Further, ALPA believes that FFDOs should never be required to remove their weapon from their person while performing the functions of an operating flightcrew member. SOPs must be rewritten to authorize these protocols and to clearly define the legal rights, duties, and protections afforded to FFDOs in following them.

Powers and Privileges to be Granted to FFDOs

Nothing in the law or FFDO SOPs should be interpreted to prohibit an FFDO from acting reasonably to prevent an act of terrorism, or otherwise to protect life in defense of the flight deck.

Because of the limited jurisdiction and mission of FFDOs, they do not require, nor do they receive, the same amount of training as federal air marshals and other federal law enforcement agents. In view of these circumstances, ALPA recommends that existing law enforcement response protocols aboard airliners be followed, with federal air marshals maintaining primary jurisdiction over incidents requiring law enforcement intervention.

FFDOs, having been properly trained and authorized to travel armed in airliner cabins, should hold a defined place in the law enforcement response continuum, following the lead of any other duly authorized federal law enforcement agent, but with authority that supersedes that of any state or local law enforcement officer traveling on board.

Nothing in the law or FFDO SOPs should be interpreted to prohibit an FFDO from acting reasonably to prevent an act of terrorism, or otherwise to protect life in defense of the flight deck. This logic must apply whether an FFDO is an operating flightcrew member or traveling in the cabin of an airliner.

Leave for Training

Scheduling issues are negatively affecting program application rates and denying the airlines the security benefits afforded by the FFDO program.

Some pilots whom the TSA has selected to attend FFDO basic training have been unable to do so because of difficulty in obtaining approved time off from their employers. Several airlines have denied their pilots' requests for unpaid leave, use of vacation time, and scheduling accommodations. Unfortunately, these scheduling issues are negatively affecting FFDO program application rates and denying the airlines the security benefits afforded by the FFDO program.

ALPA White Paper
AIR LINE PILOTS ASSOCIATION, INTERNATIONAL

Federal Flight Deck Officer Program

FFDOs provide a vital service to national security efforts that are coordinated by the Department of Homeland Security. As such, ALPA believes that, similar to the requirement placed upon employers of military reservists and members of the National Guard to grant them leave to defend the nation, airlines should be required to grant pilots time to attend FFDO basic, requalification, and recurrent training exercises. Although this leave is unpaid, it would facilitate pilots' ability to attend FFDO training and bolster this significant defensive layer in the U.S. air transportation system. Such a development will require congressional action.

Training Requirements and Locations

ALPA recommends that the TSA develop joint training exercises involving FAMs and FFDOs to facilitate an effective team approach to protecting the flight deck.

FFDO training must be conducted in a standardized, consistent fashion to provide FFDOs with the best tools, knowledge, and tactical skills needed to effectively accomplish their mission. The quality and uniformity of FFDO training are crucial factors. The training curriculum must also be readily adaptable to meet changing needs and conditions. Training updates must be easy to deploy and provided consistently.

ALPA commends the TSA for having developed and implemented an extremely effective FFDO training curriculum. Pilots graduating from FFDO basic training consistently attest to its excellence. This initial training provides FFDOs with the basic skill set necessary to perform their mission. However, for FFDOs to remain an effective force, the training program must be continually re-evaluated and updated as the threat environment evolves. Any tactic or procedure that reduces the FFDO's ability to perform his/her mission or introduces unnecessary risk must be modified or replaced and communicated.

To strengthen the FFDO program, the TSA must re-examine and improve certain key training components. Currently, basic training is supplemented by twice-a-year firearms requalification training. This component of the program must be enhanced to include a recurrent training module that offers current, in-depth tactical and intelligence training based on evolving threats. Any additional training must be consistent with and build upon the training foundation previously provided to FFDOs.

ALPA supports the concept of FFDO training sites being located where airline pilots throughout the United States can get to them easily. This goal can be accomplished by increasing the number of available training sites and strategically positioning them. While the TSA has done a relatively good job towards this end, currently no requalification sites exist in Hawaii and Alaska. FFDOs residing or based in these states must travel to the continental United States to comply with requalification requirements, usually at significant personal cost, both in terms of time and money. The TSA must correct this negative aspect of the requalification program.

ALPA has long supported the FAMS and views the FFDO program as complementary to it. Because of the commonality of certain specific mission responsibilities of FAMs and FFDOs, ALPA recommends that the TSA develop joint training exercises involving both of these federal law enforcement groups to facilitate an effective team approach to protecting the flight deck.

Currently, the FAMS is providing FFDO recurrent training at its Atlantic City, N.J., facility. While ALPA applauds the FAMS for initiating this effort, the Association recognizes that one recurrent training site will not be sufficient. The FAMS has indicated its intention to expand this training capability to additional sites strategically located throughout the United States. To provide FFDOs with ongoing training that will ensure continued successful performance of their mission will require multiple recurrent training sites. To accomplish this goal, the FAMS will need additional funding and staffing. Congress must ensure that the FFDO program is sustained through specifically appropriated funds earmarked to provide the necessary training, professional growth and sustenance of the FFDO program.

Training Costs Incurred by FFDOs

ALPA believes that, in consideration of these personal sacrifices and the resulting benefits derived by the nation and the airline industry, the TSA should reimburse FFDOs for all reasonable costs associated with participating in this program, such as travel, food, and lodging expenses.

FFDOs frequently incur significant out-of-pocket expenses to attend basic, requalification, and recurrent training. For example, costs incurred by FFDOs for basic training vary from $300 to $500. Twice-yearly firearms requalification costs average $75 per event. The recurrent training program costs range between $400 and $800 per pilot, depending on the location of the FFDO's residence.

FFDOs are willing to volunteer their energy, time, personal finances and service to enhance the security of airline operations, the aviation industry, the traveling public, and the U.S. national infrastructure. The resulting benefits derived by the nation and the airline industry are significant. ALPA believes that, in consideration of these personal sacrifices, the TSA should reimburse FFDOs for all reasonable costs associated with participating in this programs, such as travel, food, and lodging expenses.

Support of Field-Deployed FFDOs

After graduating from basic training, an FFDO is deployed on mission status without the benefit of a field training officer or frontline supervisor to help with the FFDO's transition into the realities of the assignment and to provide ongoing support. The FFDO is merely given a TSA telephone number to call if issues arise and a protected website for routine scheduling of missions and limited information-sharing. ALPA has urged the TSA to establish a more extensive communications, management, and reporting structure.

The TSA has not been fully successful in establishing and using an automated communications mechanism for the FFDO community. E-mail generally serves as the notification medium and the normal conduit by which individual FFDOs and the TSA exchange information. The secure FFDO website, while capable of being used for multiple applications, including distance learning, is normally limited to schedule planning and infrequent, brief operational messages. The TSA has not made good use of this tool to facilitate oversight and continued professional training of the FFDO community. ALPA has offered to help the FAMS rectify this situation.

FFDOs should be able to communicate with one another through authorized, appropriate, and secure means. They also should be able to provide peer support through a professional mechanism created in partnership with the TSA. Today, the TSA has no clearly defined crisis management response protocol to help FFDOs who become engaged in a significant security event. These enhancements would promote a healthy and viable organization.

Since October 2005, the FAMS has maintained responsibility for oversight of the FFDO program and has indicated its intent to provide more effective training, support, and management of FFDOs. Unfortunately, the FAMS has not clearly articulated its plan for accomplishing the needed reforms, defined the remedial process, or provided a timeline delineating when much-needed changes will be made. While the FAMS has certainly made progress in this regard, ALPA looks forward to fulfillment of this commitment.

Internal Affairs and Disciplinary Actions

A requirement for FFDOs to make statements that may be against their own interest without benefit of protection from civil or criminal liability is unacceptable. SOPs regarding internal investigations FFDOs must be properly defined, clearly communicated to the FFDO population, and followed. FFDOs must be afforded the same protections as are provided to other law enforcement officers.

FFDOs who become the subject of an internal investigation are not adequately informed of their rights, exposure to liability, procedural requirements, and a timeline for adjudication. Although this situation has not prevented pilots from applying to the FFDO program, it remains a cause for concern.

Experience has shown that FFDOs have been exposed to potentially significant penalties, including being fired by their airline, for seemingly insignificant violations of FFDO SOPs. Often, FFDOs receive no written statement of charges/allegations against them or information delineating the process/timeline required to adjudicate the matter. Usually, an FFDO is notified orally that he/she is under investigation and is instructed to surrender his/her credentials and weapon while the investigation proceeds. Long periods of time elapse with no communication back to the FFDO regarding his/her status or the progress of the inquiry.

TSA SOP's require FFDOs to cooperate with the internal investigation process, but FFDOs are provided no guidance regarding right to counsel, making statements against their own interest, or resulting potential exposure to civil or criminal liability. U.S. Supreme Court decisions provide a clear roadmap governing internal investigations of full-time law enforcement officers, particularly focusing on protections against self-incrimination. To date, no such protections have been afforded to FFDOs.

ALPA recognizes that FFDOs are not full-time law enforcement officers and that loss of their FFDO status as a result of an internal investigation will not normally affect their airline employment. However, a requirement for FFDOs to make potential statements against their own interest without benefit of protection from civil or criminal liability is unacceptable. SOP's regarding internal investigations of FFDOs must be properly defined, clearly communicated to the FFDO population, and followed. At a minimum, FFDOs must be afforded the same protections that are provided to other law enforcement officers.

ALPA White Paper
AIR LINE PILOTS ASSOCIATION, INTERNATIONAL

Federal Flight Deck Officer Program

Because the reliable presence of FFDOs would provide a predictable layer of defense against the threat of hijacking of international flights, ALPA believes that the TSA should do everything in its power to work with the U.S. Department of State to obtain agreements with foreign governments that will allow international deployment of FFDOs.

International Deployment

Many airline trips include international segments for flight crews. Under current procedures, FFDOs are authorized to fly in mission status only on domestic routes. This policy not only makes inefficient use of valuable counterterrorism assets, it can also result in significant hardship for FFDOs and airlines. If an on-call (reserve) FFDO is assigned an international flight, he/she must find a way to secure his/her weapon at his/her domicile or refuse the trip. While a number of airports have gun storage lockers available for FFDO use, they are often fully occupied or not functional. Although the TSA has advised FFDOs that airport federal security directors (FSDs) are available to help them in such situations, this help is sporadic and unreliable.

ALPA recognizes that the greatest impediment to international deployment of FFDOs is the sovereignty of foreign nations and laws that prohibit or severely limit entry of weapons into their respective territories. Notwithstanding that fact, the reality that large, widebody airliners that fly international routes present attractive targets to terrorists cannot be ignored.

Because the reliable presence of FFDOs would provide a predictable layer of defense against the threat of hijacking of international flights, ALPA believes that the TSA should do everything in its power to work with the U.S. Department of State to obtain agreements with foreign governments that will allow international deployment of FFDOs.

Cockpit Jumpseats

FFDOs often occupy cockpit jumpseats while commuting or traveling for FFDO training purposes. Current SOPs limit their ability to deploy in mission status in such circumstances. To make more efficient use of the layer of security provided by FFDOs, ALPA recommends that SOPs be modified to permit jumpseating FFDOs to be on mission status, contingent upon the approval of the pilot in command of the flight.

Captain's Authority

The presence of any law enforcement officer, including an FFDO, on an airliner in no way supersedes the clearly established authority of the captain (i.e, pilot in command), who retains ultimate command of the flight.

Captain's authority is not diminished by the presence of armed law enforcement officers aboard the airliner. However, captain's authority does not extend to preventing a federal law enforcement officer, such as a FAM or FFDO, from exercising his/her federally mandated duties.

No legislative amendments to the FFDO program should interfere with or alter captain's authority established in law.

ALPA White Paper

Federal Flight Deck Officer Program

Law Enforcement Officer Verification Card System

ALPA was involved many years ago in the Federal Aviation Administration's development of the Law Enforcement Officer Verification Card System (LEOVCS), a program designed to positively verify the identity and employment status of all armed persons transiting airport security checkpoints. The TSA has opted against installing that system. ALPA believes that LEOVCS, or an equivalent system, should be implemented as soon as practical, and that FFDOs should be screened at checkpoints in the same fashion as other armed law enforcement officers.

ALPA believes that LEOVCS, or an equivalent system, should be implemented as soon as practical, and that FFDOs should be screened at airport security screening checkpoints in the same fashion as other armed law enforcement officers.

Conclusion

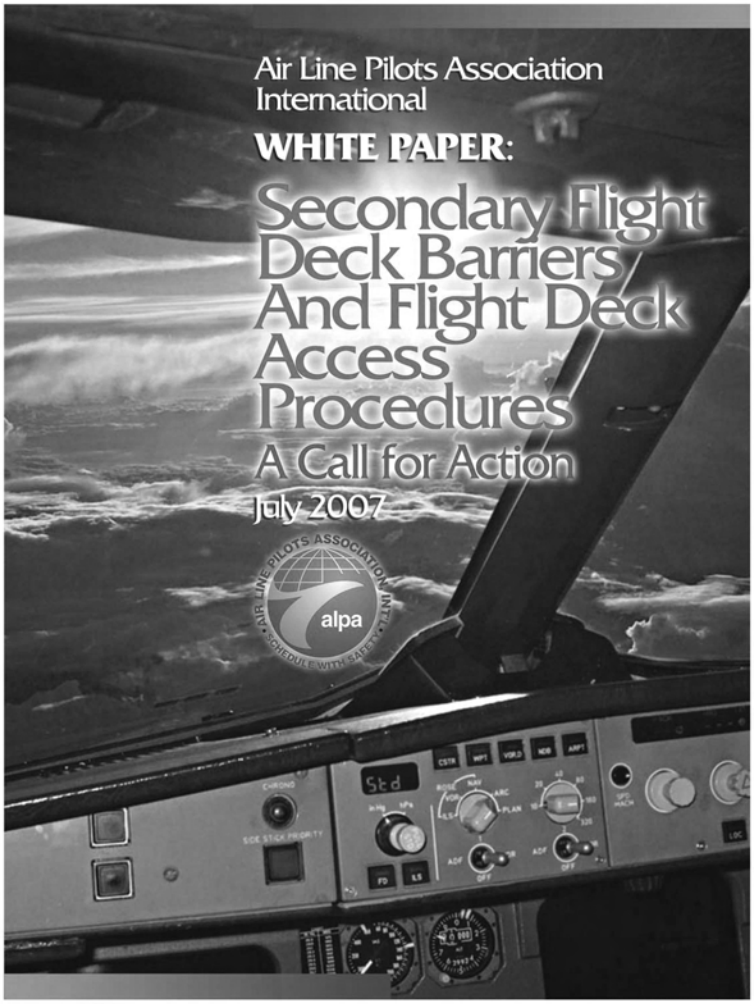
The FFDO program represents an extremely valuable asset in today's layered approach to aviation security, having been heralded as one of the most effective enhancements since the events of Sept. 11, 2001. Because of it, the United States gains great benefits from the willingness of airline pilots to make significant personal sacrifices to ensure the security of a critical component of the U.S. infrastructure.

To ensure the continued viability of the growing FFDO program, the aspects of weapons carriage, jurisdictional authority, leave and expenses for training, professional development, communications, information processes, and field management must be re-examined and improved.

ALPA appreciates the significant efforts of the TSA and the Federal Air Marshal Service in developing, deploying, and managing the FFDO program. The Association remains committed to continuing to provide its expertise to the FAMS, the TSA, and Congress to ensure the safest, most prudent, and most efficient implementation of the program possible.

The Association remains committed to continuing to provide its expertise to the FAMS, the TSA, and Congress to ensure the safest, most prudent, and most efficient implementation of the program possible.

Attachment B



ALPA WHITE PAPER

AIR LINE PILOTS ASSOCIATION, INTERNATIONAL
1625 Massachusetts Avenue, N.W., Washington, D.C. 20036
703-481-4440 • MEDIA@ALPA.ORG • WWW.ALPA.ORG

Secondary Flight Deck Barriers And Flight Deck Access Procedures

A secondary barrier, accompanied by standardized procedures for protecting the cockpit door when opened in flight, would significantly augment the fortified door and add an important layer of security to prevent hostile takeover of the cockpit.

The Air Line Pilots Association, International (ALPA), founded in 1931, represents the safety and security interests of 60,000 pilots who fly for 41 U.S. and Canadian domestic and international passenger and all-cargo airlines. Based on our considerable experience and vested interest in aircraft design and operational safety and security, we offer our views regarding secondary flight deck barriers. To learn more about ALPA, visit the Association's website, www.alpa.org.

Executive summary

Reinforced airliner cockpit doors mandated by the U.S. Congress and the Canadian Parliament after the terrorist attacks of Sept. 11, 2001, have added a valuable level of protection to airliner flight decks. Experience has proved, however, that the doors do not provide a complete solution to the problem they were intended to resolve. A secondary barrier, accompanied by standardized procedures for protecting the cockpit door when opened in flight, would significantly augment the fortified door and add an important layer of security to prevent hostile takeover of the cockpit.

ALPA and other airline industry advocates therefore urge the U.S. Congress, the FAA, the TSA, the Canadian Parliament, Transport Canada, and other appropriate U.S. and Canadian government agencies to require secondary flight deck barriers and appropriate flight deck access procedures on all airliners by Jan. 1, 2010. The secondary barriers should be able to delay, by at least 5 seconds, anyone trying to attack the cockpit.

The threat is real

Government intelligence-gathering efforts continue to indicate that terrorist organizations remain interested in hijacking airliners to use as improvised weapons of mass destruction. Despite worldwide government and industry attempts to prevent persons likely to engage in this criminal behavior from boarding airliners, individual hijacking attempts continue to occur throughout the world.

The vulnerability of flight deck security has been laid bare recently by the following hijacking incidents:

- *Oct. 3, 2006:* Turkish Airlines Flight 1476, a Boeing 737 with 113 passengers and crew members aboard, while en route from Tirana, Albania, to Istanbul, Turkey
- *Jan. 24, 2007:* Air West Flight 612, a Boeing 737 with 103 passengers and crew members aboard, while en route from Khartoum, Sudan, to El Fasher, Darfur
- *Feb. 15, 2007:* An Air Mauritanie Boeing 737 with 71 passengers and 8 crewmembers aboard, while en route from Nouakchott to Nouadhibou, Mauritania
- *April 10, 2007:* Pegasus Airlines Flight 157, a Boeing 737 with 175 passengers and 6 crew members aboard, while en route from Diyarbaker to Istanbul, Turkey

ALPA WHITE PAPER
AIR LINE PILOTS ASSOCIATION, INTERNATIONAL

Secondary Flight Deck Barriers and Flight Deck Access Procedures

PHOTO: UNITED AIRLINES

The barrier...

Each of these events involved an armed hijacker attempting to gain unauthorized access to the flight deck. In two instances, the hijackers were reported to have used firearms, though there are conflicting reports as to the type of weapons used and injuries sustained.

Operational experience with reinforced doors

After Sept. 11, 2001, the U.S. Congress and the Canadian Parliament mandated that airlines replace standard cockpit doors with hardened doors on certain types of airliners. The reinforced cockpit door has proved to be a valuable enhancement to flight deck security.

If the door remained closed and locked throughout all flight operations, flight deck security would be better assured. However, operational experience has shown that, on many flights, the fortified flight deck door does not remain closed for the entire flight. The flight crew or cabin crew members must open the cockpit door during extended operations for a variety of reasons, including crewmember coordination, meal service, and pilots' physiological needs. During this time of opening and closing, known as "door transition," the protective characteristics of the fortified door are negated, and the flight deck becomes vulnerable to attack.

Crew procedures and supplementary measures

The reinforced door is a vital element in flight deck protection, but it is not sufficient to protect the flight deck from attack. As a result, many airlines have established flight deck access procedures to ensure that door transitions are made safely and in minimal time. In addition, a number of airlines have approved and begun improvised use of onboard equipment as a supplementary, interim protective barrier whenever the reinforced door is opened in flight.

Generally, a flight attendant positions a galley/beverage cart diagonally across the aisle and monitors the cabin during the door transition. While using a galley/beverage cart in the aisle, coupled with properly executed door transition procedures, may provide an improvised method of protecting the cockpit, these combined precautions do not establish a predictably reliable system capable of significantly slowing and deterring a hijacker intent on seizing control of the flight deck.

Thus the reinforced flight deck door does not provide a complete solution for securing the flight deck.

Flight deck security in the all-cargo environment

In the unique all-cargo segment of the airline industry, many airliners, including widebody designs, operate with no cockpit doors at all, and newly manufactured cargo airliners are not required to be equipped with cockpit doors. All-cargo flight crew members do not have the support of flight attendants or U.S. Federal Air Marshals.

ALPA WHITE PAPER
AIR LINE PILOTS ASSOCIATION, INTERNATIONAL

Secondary Flight Deck Barriers and Flight Deck Access Procedures

PHOTO: UNITED AIRLINES

The barrier in position as viewed from the galley.

Because all-cargo airliners often carry supernumeraries (i.e., company employees or handlers of unique types of cargo), these flight crews are vulnerable to attack any time a flight deck door is opened in flight. Moreover, recent history has shown the ease with which stowaways can board all-cargo airliners. Terrorists or other persons with malicious intent can readily exploit this vulnerability. In fact, the TSA has publicly stated that hijacking poses the greatest threat to the all-cargo segment of the airline industry.

All-cargo airliners are operated in the same airspace as those passenger airliners that are subject to more-stringent security regulations. Cargo airliners, if commandeered, can inflict damage as severe as that caused by their passenger-carrying counterparts.

The solution: secondary barriers

Because protecting the air transportation system is critical to the national economies and defense of the United States and Canada, the security of the cockpits of passenger and all-cargo airliners must be assured. While the reinforced cockpit door has contributed greatly to accomplishing this goal, it has not provided the total solution as originally envisioned. Clearly, the reinforced door is only one component of a multifaceted system necessary for protecting the flight deck.

The solution to this security deficiency is a secondary barrier—a lightweight device that is easy to deploy and stow, installed between the passenger cabin and the cockpit door—that blocks access to the flight deck whenever the reinforced door is opened in flight. The combined system of the reinforced cockpit door and secondary barrier must be accompanied by mandatory, standardized crew procedures governing use of the secondary barrier in conjunction with the reinforced door.

Federal authorities must acknowledge the obvious vulnerabilities associated with the reinforced door and take appropriate measures to ensure that the flight decks of passenger and all-cargo airliners are protected from hostile takeover. They should assume both the oversight role and financial responsibility for designing and installing secondary barriers, working in conjunction with the aviation industry and aircraft manufacturers.

Installing and using a secondary barrier, coupled with standardized flight deck access procedures, can provide a number of security benefits to airlines:

- The secure zone between the secondary barrier and the cockpit door establishes a buffer area that gives the crew an opportunity to visually assess a perceived threat.
- The barrier allows effective interpretation of hostile intent and gives the crew critical extra seconds to react.
- Further, any attempt to breach the secondary barrier would confirm the perpetrator's hostile intent to U.S. Federal Air Marshals (FAMs), Canadian Aircraft Protective Officers (APOs), Federal Flight Deck Officers (FFDOs), and other armed law enforcement officers, plus flight attendants and passengers enlisted to help defend the airplane.

Voluntary industry movement toward designing and deploying secondary barriers and flight deck access procedures began in 2003 with

ALPA White Paper
AIR LINE PILOTS ASSOCIATION, INTERNATIONAL

Secondary Flight Deck Barriers and Flight Deck Access Procedures

PHOTO: UNITED AIRLINES

The barrier in position as viewed from the aisle.

United Airlines' installation of secondary barriers on select airplanes in its fleet, and has continued with Northwest Airlines' installation of primary flight deck barriers on its B-747F cargo fleet. ALPA commends both airlines for taking significant leadership roles on this crucial security enhancement in the absence of federal guidance or standards.

Design standards and crew procedures

Although these two U.S. major airlines have developed and installed secondary barriers, there are no agreed-upon design standards for their manufacture and installation. Similarly, no standardized procedures exist for using such secondary barriers.

The process for developing standards should incorporate criteria including, but not limited to, effectiveness, ease and cost of installation, maintenance, effect on airplane liability insurance rates, ease of operation (functionality and effect on flight and cabin crew procedures), minimal activation and stowage time, weight, flight and cabin crew safety issues related to emergency ingress/egress situations, current and future airliner design issues, and adaptability of such secondary barrier devices. Government efforts should begin with evaluating existing, approved secondary barrier designs such as those used by United Airlines.

To develop a viable product, appropriate government agencies must conduct meaningful dialogue with flight and cabin crew unions, airline managements, and airliner manufacturers. Stakeholders should agree on flight deck access procedures and then incorporate them into government-approved standard security programs for passenger and all-cargo operations. The stakeholders also should consult with the Federal Air Marshal Service, the Royal Canadian Mounted Police, and the Federal Bureau of Investigation because of the effects that installing secondary barriers and developing standard flight deck access procedures may have on operational and tactical procedures used by these law enforcement agencies.

ALPA encourages all airlines to partner with federal agencies and other stakeholders in developing the design standards and appropriate flight deck access procedures, and to equip their fleets with secondary barriers as soon as possible, but not later than Jan. 1, 2010. ALPA recommends that the secondary barrier be designed to delay, by at least 5 seconds, anyone trying to attack the flight deck. The key requirement for door-transition procedures is to ensure that the flight or cabin crew can secure the reinforced door before an attacker penetrates the secondary barrier.

Conclusion and recommendation

The reinforced cockpit door has added a valuable level of protection to the flight deck, but does not completely eliminate the opportunity for hostile takeover of the cockpit. Delaying a potential attacker by 5 seconds, via a secondary barrier, along with standardized crew procedures for flightdeck door transitions, would add greatly to the security of the flight deck. ALPA therefore urges appropriate U.S. and Canadian government agencies to require secondary flightdeck barriers and appropriate flightdeck access procedures on all airliners by Jan. 1, 2010.