



U.S. Department of Transportation
Office of the General Counsel
400 Seventh Street, S.W., Room #10428
Washington, D.C. 20590

(b) (2) High

facsimile

Date: July 9, 2003

FACSIMILE COVER SHEET

To: Shirley Miller

Agency: FAA

Telephone: (b) (2) High

Facsimile:

Message:

No. of Pages: 2 , including cover

From: Lindy Knapp
Deputy General Counsel

Telephone:

Facsimile:

(b) (6)

**U.S. Department of
Transportation**Office of the Secretary
of Transportation**GENERAL COUNSEL**400 Seventh St., S.W.
Washington, D.C. 20590**July 10, 2003**

Daniel Marcus
General Counsel
National Commission on Terrorist Attacks
Upon the United States
301 7th Street SW, Room 5125
Washington, DC 20407

Dear Dan:

This is in response to your letter of June 13, 2003 inquiring about the status of the Department of Transportation response to the Commission's Document Request No.1. This memorandum provides a summary of documents that DOT has submitted to date in response to the first document request.

Item #1: Responses were submitted on May 28, June 5 and June 9. We believe this item has been fully responded to. In addition, TSA may have additional information as indicated in the FAA's May 28 transmittal memo.

Item #2: Although not specified in the June 5 and June 9 memorandums from the FAA, the information provided by the FAA in response to Item #1 also covers this item so we believe this item has been fully responded to.

Item #3: As FAA indicated in their May 28 transmittal memo, this information primarily resides with TSA. However, there are 3 memorandums of understanding between FAA and the US Secret Service that we will be providing to the Commission.

Item #4: This item was fully responded to on May 28.

Item #5: The FAA provided radar data in text form as part of the first submission on May 28. On June 4, the Commission staff was briefed on the tracking of the four hijacked flights. Subsequently, FAA provided a CD with the same briefing (not documented in a separate memorandum by the FAA). Additionally on June 4, portions of the radar tracking for three of the hijacked flights were viewed by five staff members in the FAA's Air Traffic lab. This presentation included radar and voice communications. The FAA is following up with a transcript of the communications between our Air Traffic Control facilities that handled the flights and the communications with Department of Defense elements on September 11, 2001. We will forward the transcript to the Commission as soon as it is available. With regard to the remaining data and information that the FAA released to the NTSB following 9/11, we are in consultation with the NTSB and other agencies to determine the protocol for releasing the remaining information.

Item #6: This item was fully responded to on May 28.

Item #7: FAA submitted materials on June 5 and June 9 that address this request. Although the request was specific to FAA handling of hijacked airliners, we have included additional information on actions the FAA took as a result of lessons learned from 9/11. We are in the process of determining whether there is additional documentation that would respond to this request item. In addition to the information that has already been provided by the FAA after 9/11, the Secretary of Transportation formed Rapid Response Teams to address longer-term airport and aircraft security issues. Copies of those Rapid Response Teams' Reports are attached.

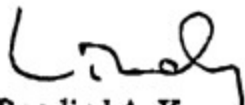
Item #8: As we have indicated previously, the documents provided to the Joint Inquiry by DOT will be provided by TSA.

We will provide outstanding documents as soon as possible for the remaining items discussed above.

Finally, we are putting together the briefings discussed in the DOT Briefing Request No. 1 and will be working on responding to DOT Document Request No. 2.

Please let me know if I can be of further assistance.

Sincerely,



Rosalind A. Knapp
Deputy General Counsel

Attachments

**News
U.S. Department of Transportation****MEETING THE AIRPORT SECURITY CHALLENGE****Report of the Secretary's Rapid Response Team on Airport Security****October 1, 2001**

Extraordinary challenges require extraordinary measures. The terrorist attacks on America of September 11, 2001 require that we reform our Nation's aviation security system in fundamental ways. On September 27, President Bush launched this process of reform by announcing his proposals for (1) an expanded federal air marshal program, (2) a \$500 million federal grant program to strengthen aircraft security, (3) federal management of airport security and screening services, and (4) pending full implementation of federal oversight of airport security, the call-up of National Guard troops by State Governors to augment existing security staff at commercial airports nationwide.

To build on the President's proposals and make the Nation's airports more secure, the Rapid Response Team has concluded that:

- Airport passenger screening must be placed under the direct control of a new federal law enforcement agency housed within the Department of Transportation.
- Relevant law enforcement and Intelligence Information must be shared on a continuing basis with those responsible for aviation security.
- New technologies must be deployed more widely to augment the aviation security program.
- Airport passenger screening and other security procedures must be strengthened to ensure that they provide adequate protection for air travelers.
- There is an urgent need to establish a nationwide program of voluntary pre-screening of passengers, together with the issuance of "smart" credentials, to facilitate expedited processing of the vast majority of air travelers and to enable security professionals to focus their resources more effectively.

This report addresses the security issues that arise at airports in connection with travel on commercial airlines.^[1] A detailed discussion of specific actions follows. A separate Rapid Response Team will report on security issues arising in connection with aircraft construction and operation.

This Team recognizes the need to achieve a balance between improving airport security and minimizing air travel disruptions. The freedom to travel not only is a basic tenet of the American way of life, but also contributes to the livelihood and economic well being of every American citizen. For this reason, as the Department of Transportation and other federal agencies work to implement the recommendations of this report, the airline and airport communities should be provided with the opportunity to participate in the design and validation of new requirements as they are formulated.

Finally, the Team wishes to underscore its conviction that the measures proposed in the pages that follow can and should be implemented in a way that is wholly consistent with America's commitment to the protection of civil rights.

RECOMMENDATIONS**FEDERALIZATION OF AVIATION SECURITY**

Recommendation 1: Establish a new federal security agency, housed within the Department of Transportation, to

BEYOND THE AIRPORT SECURITY CHALLENGE

7/8/03 1:59 PM

serve as the law enforcement arm for U.S. transportation, starting with commercial aviation.

The Rapid Response Team applauds the President's decision to place under federal control the management of passenger screening at U.S. airports. The Team also believes that this function should be vested in a new federal transportation security agency with full law enforcement authority. The agency's responsibilities for airport security would include the supervision of all functions related to airport passenger and baggage screening. The screening function would be significantly higher in quality, while preserving accessible air transportation as a competitive, vital, and essential component of our economy.

Consistent with the President's proposals, the new transportation security agency would establish new standards for security operations; would perform intensive background checks and train and test screeners and security personnel; would purchase and maintain all equipment; and would work cooperatively with other law enforcement authorities at the federal, state, and local levels.

The new security agency would hire, train, and deploy to airports throughout the Nation a cadre of uniformed federal transportation security officers. Consistent with the President's proposals, these officers would oversee and manage the full range of airport security functions to be carried out by federal or contract personnel, including but not limited to:

- screening of passengers, baggage, and aircraft;
- patrolling secure areas of the airport;
- monitoring the quality of the airport's access control;
- exercising federal arrest authority;
- training of contractor personnel in the performance of screening and selected other security functions; and
- working with law enforcement authorities at the federal, state, and local levels and serving as a key facilitator of coordination with the Department of Homeland Security.

The federal transportation security agency would also have responsibility for:

- monitoring and disseminating relevant threat information, law enforcement data, and other relevant intelligence;
- overseeing air carriers' compliance with FAA security regulations; and
- conducting background checks required of persons working at an airport.

The new security agency would provide an effective response to the perceived passenger screening and airport access inefficiencies in the present structure. In particular, the new office would be able to attract and retain a motivated corps of law enforcement and security professionals. Likewise, security background checks would be conducted in keeping with consistent federal standards, while training in security requirements and procedures would be provided on a more comprehensive, uniform basis. Most important, standards would be consistently high throughout the Nation, allowing travelers to enjoy the convenience of air travel with a heightened level of confidence in the integrity of the system.

FORMATION INTEGRATION AND SHARING

Recommendation 2: Integrate law enforcement and national security intelligence data with airline and airport systems, including passenger reservation, screening checks, employee background checks, employee and passenger identification, and access protocols to aircraft and secure areas within airports. This could be carried out under the auspices of the Office of Homeland Security.

It is time to change fundamentally the way our airports, airlines, and law enforcement and intelligence communities use, share, and process law enforcement and national security data. Doing so will provide the underpinning for (1) rapid response by airline and airport operators to terrorist threats; (2) an enhanced screening of airport and airline employees and passengers, including the more effective use of the Computer Assisted Pre-screening Passenger System; and (3) the application of new technologies for identification purposes and to enhance security access at airports.

TESTING THE AIRPORT SECURITY CHALLENGE

7/6/03 1:59 PM

Recommendation 3: All airlines and airports should designate a senior-level security officer and that officer should possess a security clearance at a level required to act on sensitive intelligence information.

Airport authorities and airlines must have a person at each airport in possession of a security clearance at a level sufficient to enable effective interaction with the law enforcement and intelligence communities and ensure that swift and decisive action is taken in response to sensitive information that is made available.

EXPLOITING BREAKTHROUGH TECHNOLOGIES

Recommendation 4: New technologies for the positive identification of passengers, airport workers and crews, detection of explosives, and more effective passenger and baggage screening should be incorporated in airport security programs as soon as practicable.

An array of new technologies exists with the potential to enhance dramatically the quality of passenger and employee identification, tracking, and verification. Similar improvements in explosive detection technologies and passenger and baggage screening are also being developed. Properly deployed, these tools can be a powerful weapon in the war against terrorism. The Rapid Response Team urges that available technologies be incorporated more widely in our airport security program as soon as practicable.

Recommendation 5: The Federal Aviation Administration should establish an Aviation Security Technology Consortium, including public and private sector participants, to identify, sponsor, and test new security-related technologies at our Nation's airports.

The Team urges the creation of an Aviation Security Technology Consortium under the auspices of the FAA – including public and private sector members – to identify, sponsor, and test new security-related technologies at our Nation's airports.

Recommendation 6: The Department of Defense should conduct an accelerated review of classified technologies with potential application to aviation security with a view to identifying and, consistent with national security requirements, declassifying applications likely to be of value.

As part of the Nation's effort to exploit new technologies in protecting aviation against terrorism, it is essential that sensitive technologies currently subject to government classification be reviewed to ensure that applications of possible relevance to the aviation security challenge are not overlooked. Where such applications hold potential promise and can be adapted without compromising national security, they should be appropriately declassified.

IMPROVED PASSENGER SCREENING AND ACCESS CONTROL

Recommendation 7: Apply the Computer Assisted Passenger Pre-Screening System (CAPPS) to all passengers.

CAPPS is a new process for analyzing information known about a passenger in the carrier's reservation system and "scoring" the passenger either as a "selectee" or a "non-selectee." This process allows the security system to focus attention on a selected population of passengers for each flight, while the majority of passengers process through the standard security system. Application of this new process to all passengers would materially strengthen overall security.

Because it is essential that all passengers be subjected to a CAPPS screening prior to boarding, the Team recommends that all passengers now be required to check in at a location where CAPPS can be applied. It is preferable, where possible, that selectee status be determined prior to the passenger's processing through a screening checkpoint. Airlines estimate, however, that 40-60 percent of passengers do not check baggage and proceed directly to boarding gates for recheck there. The configuration of many major airports is based on this pattern. Requiring all passengers to check in prior to processing through passenger screening checkpoints, therefore, is likely to clog the checkin process unacceptably at a great many locations. Accordingly, the Rapid Response Team believes that airlines and airports must work together with the FAA to find effective ways of applying CAPPS to passengers prior to their passage through screening checkpoints.

SETTING THE AIRPORT SECURITY CHALLENGE

7/8/03 1:59 PM

Recommendation 8: Each person traveling from an airport required to meet Federal Aviation Regulation Part 107 (which governs security at airports with scheduled commercial air carrier service) should be screened at an approved screening checkpoint. In addition, all carry-on items in the possession of each person traveling on a scheduled commercial air carrier should be screened at an approved screening checkpoint. This provision should apply to all air carrier employees and crews.

Under current provisions, air carrier employees, such as baggage handlers, mechanics and ticket agents, may fly as passengers without having been screened. The Team recommends that this exception be terminated immediately, and that every passenger, regardless of status, be required to pass through a screening checkpoint prior to boarding.

Recommendation 9: Institute improved processes for screening persons and carry-on items/baggage.

First and foremost, the public expects visible improvements in passenger screening. Second, the most effective way to fulfill the public's expectation and increase the probability of stopping an attack is to focus the highest level of scrutiny on those passengers most likely to pose a genuine security risk. Third, the measures employed must cover the widest possible array of threats, from handguns to explosives to knives, which may or may not be detected by metal detector.

The Rapid Response Team has recommended, in a submission restricted to official use only, ways of screening both selectees and non-selectees consistent with these basic principles.

Recommendation 10: Carry-on luggage should be limited to one carry-on bag and one personal article such as a purse or briefcase. The existing limitation on "passengers only" beyond screening checkpoints should be continued.

The enhancements recommended in this paper, particularly with respect to screening selectees, will require that more time and attention be devoted to each piece of carry-on. By limiting the number of items needing to be screened more time is made available to screen items carefully. Overall, a more thorough and less time-pressured screening will increase effectiveness.

This recommendation logically follows already enacted limitations on who may have access to sterile areas through screening checkpoints. The overriding concept is to limit the amount of screening to be done, thereby having more time to do it well.

Recommendation 11: Until the new federal transportation security agency becomes fully operational, each airport required to meet FAR Part 107 should station a fixed-post law enforcement officer or National Guard member at each screening checkpoint while it is in operation.

Currently, most screening checkpoints in the United States are staffed by contract security personnel. Stationing a uniformed officer at the Nation's screening checkpoints will immediately improve public confidence in the screening process and it will better enable timely law enforcement support of the process.

Recommendation 12: Each airport required to meet FAR Part 107 should revalidate identification and access media that provide access to secured areas of airports.

Historically, accounting for access and identification media has been difficult and an overall weakness in airport access control systems. Already underway, this action is prudent, as it simply establishes a clean baseline from which future access media and identification enhancements may be built.

Recommendation 13: Each airport, airline and related service company required to meet FAR Part 107 and 108 should begin revalidation, under federal standards, of the background and criminal history checks previously conducted on persons who have access to secured areas of the airport. This revalidation should include checking each person against a coordinated federal security database and notifying appropriate federal authorities of discrepancies or other relevant information discovered during such revalidation processes.

Under current rules, persons have been allowed access to secure areas of airports based on a review of their employment history and, only when there are unexplained gaps in employment, a criminal history check. The type of terrorist planning that was displayed on September 11 indicates that this level of check is not adequate. By checking individuals' records

SETTING THE AIRPORT SECURITY CHALLENGE

7/8/03 1:59 PM

against a database of criminal history, known terrorists or persons illegally in the United States, it is more likely that access to secured areas of airports can be protected against undesirable persons. It is important to point out that these requirements will be largely dependent on implementation of Recommendation 2 (integration of law enforcement and intelligence information).

Recommendation 14: To the extent not already accomplished subsequent to September 11, 2001, each airport operator required to meet FAR Part 107 should change codes on all access doors and re-key all lock systems. The codes should be changed within 72 hours and the re-key should be accomplished within 30 days.

Like access media and identification, lock and key control has historically been difficult for airports to manage. It is prudent to accomplish re-keying so that a new control baseline is established. Regarding access hardware that utilizes codes, compromise of the codes is another recurring problem. Codes can be easily captured by observation or even by the fact that careless employees sometimes write these codes on the wall next to the access point.

Recommendation 15: The FAA should begin reviewing airport security programs containing exclusive-use and tenant access control agreements to determine the necessity of, and reasonable time frame for modification of, such agreements in order to ensure that a single entity is responsible for security in all areas of the airport.

Currently, the diffusion of responsibility for airport security among the FAA, the airports, and airport tenants creates an unacceptable level of fragmentation and potential loss of control over security management. Some fixed-based operator tenants, for example, do not have security personnel, resulting in weak or little monitoring of access to secured areas.

HARPENING THE FOCUS OF AIRPORT SECURITY

Recommendation 16: There is an urgent need to establish a voluntary means by which passengers might submit to an effective pre-screening regimen and thereby qualify for more expedited processing.

As passenger volume returns to normal levels, more efficient ways of moving passengers through the security system to the aircraft will be required. The Team believes that there is an urgent need to establish a nationwide program for the voluntary pre-screening of passengers, together with the issuance of "smart" credentials (taking advantage of biometric and other emerging technologies to validate personal identity). Passengers whose identities and backgrounds have been validated in advance through such a program could be processed, upon presentation of their credentials, through a less intense security process, enabling security professionals to focus their resources more effectively. Even prior to the establishment of such a program, the use of U.S. passports as a discriminator should be considered as a possible means of facilitating the passenger screening process. These approaches would streamline passenger screening without compromising security requirements.

Issues arising in connection with general aviation, including the operation of corporate aircraft, are beyond the scope of this report. The Team recommends, however, that a similar initiative be undertaken to explore ways of further enhancing the security of general aviation facilities and operations.



News
U.S. Department of Transportation

MEETING THE AIRCRAFT SECURITY CHALLENGE

Report of the Secretary's Rapid Response Team on Aircraft Security

October 1, 2001

The threat to aviation safety has changed, and so must our response. The events of September 11 changed forever our concepts of appropriate aviation safety. The use of a hijacked aircraft as a weapon requires a new strategy to ensure that the crew always retains control of the aircraft.

To combat the new threat and restore public confidence in commercial aviation, this report documents our consideration of changes to aircraft design and operation. Augmented by the suggestions and recommendations received from all sources, one or more of the following goals: 1) to deter the hijack plan, making it too difficult, expensive or undesirable to use aviation as a weapon of terror; 2) to deny access to the flight deck by any threat; 3) to delay access to the flight deck, allowing the crew time to take protective measures; 4) and to recover control through aggressive crew response.

To build on the President's proposals and make the Nation's aircrafts secure, the Rapid Response Team has concluded that:

- Some appropriate flight deck barrier device must be approved and installed in the entire U.S. fleet and future design of flight deck doors must meet newly determined requirements.
- Procedural changes must be made at all airlines regarding identification and access of all personnel to the flight deck.
- Airline industry, unions, and FAA should redesign security training with possible implementation of defensive capabilities to address newly-identified threats, incorporate changes into the annual curriculum, and provide security training to all crewmembers.
- Each airline, in cooperation with the FAA or other government entities must develop a delivery system to provide government security advisories to crewmembers in a timely manner.
- A task force should determine the necessary modifications to assure continuous transmission of a transponder signal.
- All airlines, pilots and the FAA should jointly identify procedures in pilot training that could be adapted in an attempted hijacking.

This report addresses the security issues that arise at aircrafts in connection with travel on commercial airlines. A detailed discussion of specific actions follows.

A separate Rapid Response Team will report on security issues arising in connection with aircraft construction and operation.

Finally, the Team wishes to underscore its conviction that the measures proposed in the pages that follow can and should be implemented in a way that is wholly consistent with America's commitment to the protection of civil rights.

RECOMMENDATIONS

TESTING THE AIRCRAFT SECURITY CHALLENGE

7/8/03 1:59 PM

FLIGHT DECK DOOR DESIGN

Recommendation 1: We recommend that some appropriate barrier device be approved, and installation begin within 30 days. Installation throughout the entire U.S. fleet should be completed in 90 days. We recommend that FAA enable the installation of these devices through urgent regulatory action that provides the airlines with a simple, expedited method for approval and installation.

The multiple attacks of September 11, 2001, require that changes be made to the flight deck door that will deny access to an intruder. The safety requirements related to rapid decompression and emergency access, however, must be considered. Flight deck doors on U.S. airline aircraft were designed principally to ensure privacy, so that pilots could focus on their normal duties, uninterrupted by activity in the passenger cabin. Doors were not designed to meet significant security threats such as small arms fire or shrapnel, or the use of blunt force to enter the flight deck.

The prevention of unauthorized access can be improved by the simple addition and use of a deadbolt, a cross-bar, a net or other barrier devices. Our discussions and consultations with other aviation experts indicate that this installation on any individual aircraft can typically be accomplished overnight.

Besides affording an orderly work environment for the flight crew, flight deck doors have other important safety characteristics. Current design standards require that the door must not hinder emergency exit from the flight deck or impede rescue efforts into the flight deck after an accident.

Current doors are designed to ensure that rapid decompression does not cause a failure, which could have catastrophic effects on the aircraft. Such a failure is theoretically possible in such an event, if the pressure cannot be equalized between the flight deck and the cabin in an expeditious manner. Preliminary research indicates that a rapid decompression on the flight deck side of the door has a low historical occurrence. This research has revealed no accidents caused by a rapid decompression in the flight deck. This may be because the decompressions have not been rapid enough or the venting method worked as designed.

The addition of a deadbolt or another barrier may hinder crew exit, rescue, and the venting that the door's original design provided. Given the newly identified security risks, we recommend the FAA allow the use of a deadbolt or other barrier device, in the short-term, until the impact of these devices on decompression and rescue/exit can be determined and an alternative approach is designed.

Recommendation 2: We recommend that the industry identify and address the risks regarding rapid decompression and exit and rescue associated with the barrier devices that have been installed. Within 6 months, steps should be taken to accomplish the following:

- (1) Approve a door design to ensure:
 - adequate venting of a closed and locked flight deck door in the event of a rapid depressurization in the flight deck area. Venting may involve provision of either a venting means or release of the door locking mechanism,
 - in the event of an emergency, exit and rescue of the flight crew, and
 - barrier against intrusion.
- (2) Provide a barrier against access by an intruder through the venting feature of those flight deck doors having vents.

Within 1 year from approval of the door design, conduct a retrofit of the entire U.S. fleet of aircraft.

There may be more permanent and effective solutions that require longer time for implementation. The current flight deck door and associated bulkhead are not designed to minimize or mitigate the negative impacts from breaches caused by blunt force, ballistics, fragmentation, or other explosive effects.

Strengthening of the flight deck door can be divided into the following areas: (1) Improved locking, hinge, door handle, and door frame integrity; and (2) Using specialized materials to mitigate the catastrophic effects from ballistic, fragmentation,

SETTING THE AIRCRAFT SECURITY CHALLENGE

7/9/03 1:59 PM

and explosives devices attacks. A design and performance specification with specific design requirements must be developed and approved which would include identification of the amount of load(s) the door and bulkhead must sustain from an attack and take into account the force that can be expected in an explosive decompression.

Recommendation 3: We recommend that ongoing work in the Aviation Rulemaking Advisory Committee Design for Security Harmonization Working Group be completed within 60 days, with respect to door design standards.

Safety considerations must address flight crew evacuations, venting, or an emergency crew response by flight attendants if one or all of the flight deck crew become incapacitated. There have been situations where a flight attendant was able to pull an incapacitated pilot from the controls and allow the other pilot to fly the aircraft safely to the ground.

Recommendation 4: We recommend that a future design of the doors meet the requirements of rapid decompression, flight crew rescue and exit, and protection from intrusion caused by blunt force, ballistics, fragmentation, or other explosive effects. The new design should be required for new aircraft types. We recommend that as many elements of the new design as practical be retrofitted into the fleet.

Another strategy for controlling access on some aircraft in the longer term is a mantrap, which is a set of two doors that requires the person to enter the first while the second is closed. The person cannot pass through the second door until the first door is closed. This system provides security in at least three ways. It makes it difficult to forcibly gain entry by knocking down a single door, it allows time to evaluate the person in the mantrap before releasing him or her through the second door, and it allows entry of only one person at a time. This design will have limited applicability to most aircraft in the U.S. fleet because, for example, the passenger entry door is too close to the flight deck to accommodate this design.

LIGHT DECK ACCESS

Recommendation 5: We recommend that these flight deck procedural changes be made at all airlines within 30 days.

With an immediate goal of adding barriers to the flight deck, we must address access to the flight deck and how it will be controlled. Since the events of September 11, airlines and their pilots and flight attendants have implemented their own procedures, which include:

- Prohibiting passengers from loitering at the forward lavatory and galley areas
- Leaving curtains/dividers open between cabins to allow for unobstructed views
- Strictly enforcing seatbelt signs
- Reinforcing crew coordination to facilitate immediate reporting of suspicious activities to other crewmembers
- Suspending pre-flight beverage service during the passenger boarding process to allow flight attendants to focus on passenger boarding
- Requiring the forward lavatory and the interphone to be operational for dispatch
- Positively identifying those entering the flight deck, using peepholes, codewords, or other similar methods
- Putting the jumpseat in the down position during flight if doing so inhibits access to the flight deck

If the flight deck no longer readily accessible to flight attendants, they must have a method for immediate notification to the flight deck during a suspected threat in the cabin. On receipt of such a warning, the pilot would check to make sure that the flight deck door is secure and begin immediate landing procedures. Consideration should be given to systems that might be installed in the aircraft as well as a device that could be carried by a crewmember. In those aircraft equipped with an automated evacuation alarm system, it may in the near term be an effective tool for such notification.

Recommendation 6: We recommend that industry develop a plan of feasible alternatives for emergency warnings within 30 days.

Under Security Directives already issued, airlines have restricted use of the jumpseats aboard their aircraft to their own pilots and flight engineers, and FAA inspectors. For the short term, these restrictions should be endorsed and continued. Qualified flight deck personnel in jumpseats provide safety and security benefits to the crew and passengers. The extra person assists the flight deck crew in many ways. That person is an extra set of eyes, ears, and hands, and may be able to take action for the crew while the crew flies the aircraft.

Some airlines have instituted additional screening of pilots from other airlines and are accommodating them by seating

SETTING THE AIRCRAFT SECURITY CHALLENGE

7/8/03 1:59 PM

them in the passenger cabin on space-available basis. We agree that improved screening should be required until credential verification can be improved, consisting of identification check before boarding the aircraft and again after boarding the aircraft, by the flight crew. A simple question and answer technique is recommended. Additionally, jumpseat occupants should display conspicuously a picture identification at all times on the aircraft.

Recommendation 7: We recommend that airlines and pilots unions develop procedures that will allow gate and flight deck personnel to verify the credentials of a non-company pilot or flight engineer who asks to occupy a jumpseat within 6 months.

On the long-term automated or other systems should be considered to accomplish positive identification of all flight crewmembers before entering the aircraft.

Recommendation 8: We recommend FAA and industry define requirements for an automated system to validate, in real time, the identities of persons with legitimate access to the aircraft, within 6 months. (Universal access identification). Implementation will be based on those requirements, when defined.

There is consensus that cameras to monitor and view the area outside the flight deck door may add value. There should be continuous lighting outside the flight deck door for visibility, as well as to provide lighting for cameras. However, placement of a monitor in the limited space on the flight deck is a challenge. While there may be value in video or audio systems which provide information about activities throughout the cabin, we have no consensus on whether or how to proceed with this technology.

Recommendation 9: We recommend that industry evaluate the use of cameras and lighting outside the flight deck door within 6 months.

DEFENSIVE CAPABILITIES IN CABIN AND FLIGHT DECK AREAS

Recommendation 10: We recommend industry work with the FAA to evaluate these factors and make recommendations for personal protection within 6 months. We recommend the implementation of defensive capabilities in accordance with the recommendations of the evaluation, within 1 year of receiving the recommendation.

We support the notion of crewmembers using non-lethal defensive capabilities in the cabin area and on the flight deck in back emergencies. This is a new approach to aircraft security, provoked by the attacks of September 11th. Our proposed security strategy would require that the flight crew door remain locked during a suspected security threat, leaving flight attendants with the responsibility to address all cabin disturbances without the help of the flight deck crew. The crewmembers should have access to non-lethal devices and specific self-defense training.

In the case of non-lethal devices, there is consensus that the goal of such devices is to deter any terrorist plan, deny access to the flight deck, retain control in the cabin, or if necessary recover control on the flight deck. There is no clear consensus on what type or how many non-lethal devices should be placed on the aircraft or who should have access to such devices. However, ALPA recommends installation of stun guns on the flight deck. To reach consensus, the following factors must be evaluated:

- The appropriate type(s) of non-lethal defensive capabilities and the relative effectiveness of each
- Domestic and international rules and laws governing the use of non-lethal protective devices
- Training and qualifying for all crewmembers in the use of such devices
- Weapons control (in a sealed/locked compartment on board the aircraft) and strict accountability procedures
- Standard operating procedures to maintain control of the situation after the device has been used
- Recurring maintenance and inspection of the devices
- Preventing access to these devices by passengers

Recommendation 11: ALPA recommends the FBI present reasons for or against its proposal to arm pilots.

On lethal weapons, the Air Line Pilots Association (ALPA) has taken a public position that a volunteer program be established with specific guidelines for arming pilots in flight. Other members of the task force have identified numerous

MEETING THE AIRCRAFT SECURITY CHALLENGE

7/8/03 1:59 PM

issues requiring resolution before consideration is given to arming the pilots. These issues should be considered to determine whether they can be overcome.

SECURITY TRAINING AND DELIVERING INFORMATION

Recommendation 12: We recommend industry, unions, and FAA redesign security training to address newly-identified threats within 30 days, incorporate changes into the annual curriculum within 60 days, and provide security training to all crewmembers within 6 months after updating the curriculum.

Security training is recognized as outdated in respect to today's threats. Both initial and recurrent training programs must be rapidly modernized and delivered to all crewmembers reflecting current threat information. As a minimum, this new training should prepare crewmembers to identify and understand the different levels and types of threats to the safe passage of crew, passengers, and aircraft. Development of this training should use at a minimum the expertise of law enforcement organizations and professionals familiar with hijacking situations.

Recommendation 13: We recommend that each airline, in cooperation with the FAA or other Government entities, develop within 60 days a delivery system or procedure to provide Government security advisories to crewmembers in a timely manner, including immediate threat information to affected aircraft in flight.

A related issue is the delivery of relevant security information to crewmembers and other affected personnel in a timely manner. For international operations, there is a requirement that crew briefing include relevant security threat information. The same practice should be applied to U.S. domestic operations. We need a delivery system to permit crewmembers and other appropriate persons to receive the latest security advisories, as needed. Airline dispatchers must take on the responsibility to forward all immediate threat information to affected aircraft in flight. The system should take advantage of available technology for distribution of this information.

CABIN SEARCH PROCEDURES

Recommendation 14: We recommend the FAA provide more guidance on the conduct of cabin searches within 30 days. Airlines will continue to conduct the cabin search and to provide sufficient time and training for those personnel. No cabin search duties should be assigned to flight or cabin crew.

Recent security directives require cabin search procedures to minimize risk. Current procedures do not guarantee that those conducting cabin searches are trained adequately on best practices and use of the most recent technology. We are concerned that access to the aircraft between the time the cabin search is conducted and flight is not restrictive enough. We endorse the recently introduced FAA Security Directives requiring cabin search procedures. However, there is a need for additional training for those personnel conducting cabin searches.

Recommendation 15: We concur with the recommendation of the Airport Security Team to develop a new Federal security agency and we recommend that the new agency be responsible for conducting searches of aircraft cabins.

As a long-term option, we believe this task should be assigned to some sort of Federal security force. Creating such a force would avoid the need to assign additional responsibilities to current carrier personnel who may not be as familiar with dangerous items or who may be performing other duties under limited time constraints.

UNRESPONDERS

Recommendation 16: We recommend the creation of an FAA-industry task force to determine the necessary modifications to assure continuous transmission of a hijack signal, even if the flight deck-selected code or function is shut off. Recommended action is to be defined within 30 days.

SETTING THE AIRCRAFT SECURITY CHALLENGE

7/8/03 1:59 PM

One lesson from the attacks of September 11th is the importance of ensuring continuous transponder communication with air traffic control (ATC) following a hijacking. Without the transponder switch in a fully active position, ATC can track an aircraft only by primary radar, which does not indicate aircraft identity and altitude. The loss of this information causes other aircraft to lose awareness of the flight in progress.

While it is possible that a major redesign could be required, we have learned of possible modifications that could be accomplished more quickly. The task force should examine all alternatives that would allow the ability to set and lock-in the hijacking code so that the hijacker cannot disable it; a panic button that initiates the hijacking code in an emergency situation; and an independent transponder that cannot be disabled by the hijacker.

AIRCRAFT DEFENSIVE METHODS

Recommendation 17: We recommend that within 30 days, airlines, pilots, and the FAA should jointly identify procedures in pilot training, including depressurization and rapid descent, that could be adapted in an attempted hijacking to control a hijacker.

We have received many suggestions regarding the use of aircraft defensive maneuvers as a tactic to thwart a hijacking. After industry discussion, we feel that these tactics should be used only as a last resort. While we do not openly recommend it, we acknowledge that aircraft defensive maneuvering and aggressive use of cabin pressure systems may be beneficial under certain extreme situations. Since limits in aircraft performance and pilot capabilities may prohibit or reduce the use or limit the effectiveness of such methods, any proposals must be validated for effectiveness and feasibility before implementation.