



## **The Aviation Security System and the 9/11 Attacks**

### ***Staff Statement No. 3***

Members of the Commission, your staff has developed initial findings on how the individuals who carried out the 9/11 attacks defeated the civil aviation security system of the United States. We continue our investigation into the status of civil aviation security today and for the future. These findings and judgments may help your conduct of today's public hearing and will inform the development of your recommendations.

The findings and judgments we report today are the results of our work so far. We remain ready to revise our understanding of these topics as our work continues. This staff statement represents the collective effort of the Aviation and Transportation Security Team.

Our staff was able to build upon investigative work that has been conducted by various agencies, including the Federal Bureau of Investigation. The Department of Homeland Security's Transportation Security Administration is fully cooperating with our investigators, as are the relevant airlines and the Federal Aviation Administration.

Before September 11, 2001, the aviation security system had been enjoying a period of relative peace. No U.S. flagged aircraft had been bombed or hijacked in over a decade. Domestic hijacking in particular seemed like a thing of the past, something that could only happen to foreign airlines that were less well protected.

The public's own "threat assessment" before September 11 was sanguine about commercial aviation safety and security. In a Fox News/Opinion Dynamics survey conducted at the end of the 1990s, 78 percent cited poor maintenance as "a greater threat to airline safety" than terrorism.

Demand for air service was strong and was beginning to exceed the capacity of the system. Heeding constituent calls for improved air service and increased capacity, Congress focused its legislative and oversight attention on measures to address these problems, including a "passenger bill of rights" to assure a more efficient and convenient passenger experience.

The leadership of the Federal Aviation Administration (FAA) also focused on safety, customer service, capacity and economic issues. The agency's security agenda was focused on efforts to implement a three-year-old Congressional mandate to deploy explosives detection equipment at all major airports and complete a nearly five-year-old rulemaking effort to improve checkpoint screening.

This staff statement will not address certain security performance issues leading up to 9/11 at the airports from which the hijacked planes departed. Such work is still ongoing. It should be noted that the airports themselves did not have operational or enforcement jurisdiction over checkpoint screening operations. Passenger prescreening and checkpoint screening, based on regulations from the FAA, were the responsibility of the air carriers. Nevertheless, airport authorities do play a key role in the overall civil aviation security system.

### **Civil Aviation Security Defenses**

Before September 11, federal law required the FAA to set and enforce aviation security policies and regulations that would “protect passengers and property on an aircraft operating in air transportation or intra-state air transportation against an act of criminal violence or aircraft piracy.” The layered system, one that recognized that no single security measure was flawless or impenetrable, was designed to provide a greater number of opportunities to foil those intending to do such violence.

The Civil Aviation Security system in place on September 11 was composed of seven layers of defense including:

- intelligence;
- passenger prescreening;
- airport access control;
- passenger checkpoint screening;
- passenger checked baggage screening;
- cargo screening; and
- on-board security.

The civil aviation security system in place on September 11 no longer exists. We will document serious shortcomings in that system’s design and implementation that made the 9/11 hijackings possible. We want to make clear that our findings of specific vulnerabilities and shortcomings do not necessarily apply to the current system.

Two of the layers of defense—checked baggage screening and cargo security—are not relevant to the 9/11 plot. They are not addressed in this statement. A third layer, airport access control, is still under investigation and also will not be addressed in detail. Compelling evidence, including videotape of hijackers entering through checkpoint screening stations, suggests that the hijackers gained access to the aircraft on September 11 through passenger checkpoints. What we do know is that the hijackers successfully evaded or defeated the remaining four layers of the security system.

### **The Enemy View**

We approach the question of how the aviation security system failed on September 11 by starting from the perspective of the enemy, asking, “What did al Qaeda have to do to complete its mission?”

Some time during the late 1990s, the al Qaeda leadership made the decision to hijack large, commercial, multi-engine aircraft and use them as a devastating weapon as opposed to hijacking a commercial aircraft for use as a bargaining tool. To carry out that decision would require unique skill sets:

- terrorists trained as pilots with the specialized skill and confidence to successfully fly large, multi-engine aircraft, already airborne, into selected targets;
- tactics, techniques, and procedures to successfully conduct in-flight hijackings; and
- operatives willing to die.

To our knowledge, 9/11 was the first time in history that terrorists actually piloted a commercial jetliner in a terrorist operation. This was new. This could not happen overnight and would require long term planning and sequenced operational training.

The terrorists had to determine the tactics and techniques needed to succeed in hijacking an aircraft within the United States. The vulnerabilities of the U.S. domestic commercial aviation security system were well advertised through numerous unclassified reports from agencies like the General Accounting Office and the Department of Transportation's Inspector General. The news media had publicized those findings.

The al Qaeda leadership recognized the need for more specific information. Its agents observed the system first-hand and conducted surveillance flights both internationally and within the United States. Over time, this information allowed them to revise and refine the operational plan. By the spring of 2001, the September 11 operation had combined intent with capabilities to present a real and present threat to the civil aviation system. As long as operational security was maintained, the plan had a high probability of success in conducting multiple, near simultaneous attacks on New York City and Washington, DC.

Let us turn now to a more specific look at the security system in place on September 11 related to anti-hijacking.

### **Intelligence**

The first layer of defense was intelligence. While the FAA was not a member of the U.S. Intelligence Community, the agency maintained a civil aviation intelligence division that operated 24 hours per day. The intelligence watch was the collection point for a flow of threat related information from federal agencies, particularly the FBI, CIA, and State Department. FAA intelligence personnel were assigned as liaisons to work within these three agencies to facilitate the flow of aviation related information to the FAA and to promote inter-departmental cooperation. The FAA did not assign liaisons to either the National Security Agency or the Defense Intelligence Agency but maintained intelligence requirements with those agencies.

Intelligence data received by the FAA went into preparing Intelligence Case Files. These files tracked and assessed the significance of aviation security incidents, threats and emerging issues. The FAA's analysis of this data informed its security policies,

including issuance of FAA Information Circulars, Security Directives, and Emergency Amendments. Such Security Directives and Emergency Amendments are how the FAA ordered air carriers and/or airports to undertake certain extraordinary security measures that were needed immediately above the established baseline.

While the staff has not completed its review and analysis as to what the FAA knew about the threat posed by al Qaeda to civil aviation, including the potential use of aircraft as weapons, we can say:

First, no documentary evidence reviewed by the Commission or testimony we have received to this point has revealed that any level of the FAA possessed any credible and specific intelligence indicating that Usama Bin Ladin, al Qaeda, al Qaeda affiliates or any other group were actually plotting to hijack commercial planes in the United States and use them as weapons of mass destruction.

Second, the threat posed by Usama Bin Ladin, al Qaeda, and al Qaeda affiliates, including their interest in civil aviation, was well known to key civil aviation security officials. The potential threat of Middle Eastern terrorist groups to civil aviation security was acknowledged in many different official FAA documents. The FAA possessed information claiming that associates with Usama Bin Ladin in the 1990s were interested in hijackings and the use of an aircraft as a weapon.

Third, the potential for terrorist suicide hijacking in the United States was officially considered by the FAA's Office of Civil Aviation Security dating back to at least March 1998. However in a presentation the agency made to air carriers and airports in 2000 and early 2001 the FAA discounted the threat because, "fortunately, we have no indication that any group is currently thinking in that direction."

It wasn't until well after the 9/11 attacks that the FAA learned of the "Phoenix EC"—an internal FBI memo written in July of 2001 by an FBI agent in the Phoenix field office suggesting steps that should be taken by the Bureau to look more closely at civil aviation education schools around the country and the use of such programs by individuals who may be affiliated with terrorist organizations.

Fourth, the FAA was aware prior to September 11, 2001, of the arrest of Zacarias Moussaoui in Minnesota, a man arrested by the INS in August of 2001 following reports of suspicious behavior in flight school and the determination that he had overstayed his visa waiver period. Several key issues remain regarding what the FAA knew about Moussaoui, when they knew it, and how they responded to the information supplied by the FBI, which we are continuing to pursue.

Fifth, the FAA did react to the heightened security threat identified by the Intelligence Community during the summer of 2001, including issuing alerts to air carriers about the potential for terrorist acts against civil aviation. In July 2001, the FAA alerted the aviation community to reports of possible near-term terrorist operations...particularly on the Arabian Peninsula and/or Israel. The FAA informed the airports and air carriers that

it had no credible evidence of specific plans to attack U.S. civil aviation. The agency said that some of the currently active groups were known to plan and train for hijackings and had the capability to construct sophisticated improvised explosive devices concealed inside luggage and consumer products. The FAA encouraged all U.S. Carriers to exercise prudence and demonstrate a high degree of alertness.

Although several civil aviation security officials testified that the FAA felt blind when it came to assessing the domestic threat because of the lack of intelligence on what was going on in the American homeland as opposed to overseas, FAA security analysts did perceive an increasing terrorist threat to U.S. civil aviation at home. FAA documents, including agency accounts published in the Federal Register on July 17, 2001, expressed the FAA's understanding that terrorist groups were active in the United States and maintained an historic interest in targeting aviation, including hijacking. While the agency was engaged in an effort to pass important new regulations to improve checkpoint screener performance, implement anti-sabotage measures, and conduct ongoing assessments of the system, no major increases in anti-hijacking security measures were implemented in response to the heightened threat levels in the spring and summer of 2001, other than general warnings to the industry to be more vigilant and cautious.

Sixth, the civil aviation security system in the United States during the summer of 2001 stood, as it had for quite some time, at an intermediate aviation security alert level—tantamount to a permanent Code Yellow. This level, and its corresponding security measures, was required when:

Information indicates that a terrorist group or other hostile entity with a known capability of attacking civil aviation is likely to carry out attacks against U.S. targets; or civil disturbances with a direct impact on civil aviation have begun or are imminent.

Without actionable intelligence information to uncover and interdict a terrorist plot in the planning stages or prior to the perpetrator gaining access to the aircraft in the lead-up to September 11, 2001, it was up to the other layers of aviation security to counter the threat.

We conclude this section with a final observation. The last major terrorist attack on a U.S. flagged airliner had been with smuggled explosives, in 1988, in the case of Pan Am 103. The famous Bojinka plot broken up in Manila in 1995 had principally been a plot to smuggle explosives on airliners. The Commission on Aviation Safety and Security created by President Clinton in 1996, named the Gore Commission for its chairman, the Vice President, had focused overwhelmingly on the danger of explosives on aircraft. Historically, explosives on aircraft had taken a heavy death toll, hijackings had not. So, despite continued foreign hijackings leading up to 9/11, the U.S. aviation security system worried most about explosives.

## **Prescreening**

If intelligence fails to interdict the terrorist threat, passenger prescreening is the next layer of defense. Passenger prescreening encompasses measures applied prior to the passenger's arrival at the security checkpoint. Prescreening starts with the ticketing process, and generally concludes with passenger check-in at the airport ticket counter.

The hijackers purchased their tickets for the 9/11 flights in a short period of time at the end of August 2001, using credit cards, debit cards, or cash. The ticket record provides the FAA and the air carrier with passenger information for the prescreening process.

The first major prescreening element in place on 9/11 was the FAA listing of individuals known to pose a threat to commercial aviation. Based on information provided by the Intelligence Community, the FAA required air carriers to prohibit listed individuals from boarding aircraft or, in designated cases, to assure that the passenger received enhanced screening before boarding. None of the names of the 9/11 hijackers were identified by the FAA to the airlines in order to bar them from flying or subject them to extra security measures. In fact, the number of individuals subject to such special security instructions issued by the FAA was less than 20 compared to the tens of thousands of names identified in the State Department's TIPOFF watch list that we discussed yesterday.

The second component of prescreening was a program to identify those passengers on each flight who may pose a threat to aviation. In 1998, the FAA required air carriers to implement a FAA-approved computer-assisted passenger prescreening program (CAPPS) designed to identify the pool of passengers most likely in need of additional security scrutiny. The program employed customized, FAA-approved criteria derived from a limited set of information about each ticketed passenger in order to identify "selectees."

FAA rules required that the air carrier only screen each selectee's checked baggage for explosives using various approved methods. However, under the system in place on 9/11, selectees—those who were regarded as a risk to the aircraft—were not required to undergo any additional screening of their person or carry-on baggage at the checkpoint.

The consequences of selection reflected FAA's view that non-suicide bombing was the most substantial risk to domestic aircraft. Since the system in place on 9/11 confined the consequences of selection to the screening of checked bags for explosives, the application of CAPPS did not provide any defense against the weapons and tactics employed by the 9/11 hijackers.

On American Airlines Flight 11, CAPPS chose three of the five hijackers as selectees. Since Waleed al Shehri checked no bags, his selection had no consequences. Wail al Shehri and Satam al Suqami had their checked bags scanned for explosives before they were loaded onto the plane.

None of the Flight 175 hijackers were selected by CAPPS.

All five of the American Airlines Flight 77 hijackers were selected for security scrutiny. Hani Hanjour, Khalid al Mihdhar, and Majed Moqed were chosen via the CAPPs criteria, while Nawaf al Hazmi and Salem al Hazmi were made selectees because they provided inadequate identification information. Their bags were held until it was confirmed that they had boarded the aircraft.

Thus, for hijacker selectees Hani Hanjour, Nawaf al Hazmi, and Khalid al Mihdhar, who checked no bags on September 11, there were no consequences for their selection by the CAPPs system. For Salem Al-Hazmi, who checked two bags, and Majed Moqed, who checked one bag, the sole consequence was that their baggage was held until after their boarding on Flight 77 was confirmed.

Ahmad al Haznawi was the sole CAPPs selectee among the Flight 93 hijackers. His checked bag was screened for explosives and then loaded on the plane.

### **Checkpoint Screening**

With respect to checkpoint screening, Federal rules required air carriers “to conduct screening...to prevent or deter the carriage aboard airplanes of any explosive, incendiary, or a deadly or dangerous weapon on or about each individual’s person or accessible property, and the carriage of any explosive or incendiary in check baggage.” Passenger checkpoint screening is the most obvious element of aviation security.

At the checkpoint, metal detectors were calibrated to detect guns and large knives. Government-certified x-ray machines capable of imaging the shapes of items possessing a particular level of acuity were used to screen carry-on items. In most instances, these screening operations were conducted by security companies under contract with the responsible air carrier.

As of 2001 any confidence that checkpoint screening was operating effectively was belied by numerous publicized studies by the General Accounting Office and the Department of Transportation’s Office of Inspector General. Over the previous twenty years they had documented repeatedly serious, chronic weaknesses in the systems deployed to screen passengers and baggage for weapons or bombs. Shortcomings with the screening process had also been identified internally by the FAA’s assessment process.

Despite the documented shortcomings of the screening system, the fact that neither a hijacking nor a bombing had occurred domestically in over a decade was perceived by many within the system as confirmation that it was working. This explains, in part, the view of one transportation security official who testified to the Commission that the agency thought it had won the battle against hijacking. In fact, the Commission received testimony that one of the primary reasons to restrict the consequences of CAPPs “selection” was because officials thought that checkpoint screening was working.

The evolution of checkpoint screening illustrates many of the systemic problems that faced the civil aviation security system in place on 9/11. The executive and legislative branches of government, and the civil aviation industry were highly reactive on aviation security matters. Most of the aviation security system's features had developed in response to specific incidents, rather than in anticipation. Civil aviation security was primarily accomplished through a slow and cumbersome rulemaking process—a reflection of the agency's conflicting missions of both regulating and promoting the industry. A number of FAA witnesses said this process was the “bane” of civil aviation security. For example, the FAA attempted to set a requirement that it would certify screening contractors. The FAA Aviation Reauthorization Act of 1996 directed the FAA to take such action, which the 1997 Gore Commission endorsed. But the process of implementing this action had still not been completed by September 11, 2001.

Those are systemic observations. But, to analyze the 9/11 attack, we had to focus on which items were prohibited and which were allowed to be carried into the cabin of an aircraft. FAA guidelines were used to determine what objects should not be allowed into the cabin of an aircraft. Included in the listing were knives with blades 4 inches long or longer and/or knives considered illegal by local law; and tear gas, mace, and similar chemicals.

These guidelines were to be used by screeners, to make a reasonable determination of what items in the possession of a person should be considered a deadly or dangerous weapon. The FAA told the air carriers that common sense should prevail.

Hence the standards of what constituted a deadly or dangerous weapon were somewhat vague. Other than for guns, large knives, explosives and incendiaries, determining what was prohibited and what was allowable was up to the common sense of the carriers and their screening contractors.

To write out what common sense meant to them, the air carriers developed, through their trade associations, a Checkpoint Operations Guide. This document was approved by the FAA. The edition of this guide in place on September 11, 2001, classified “box cutters,” for example as “Restricted” items that were not permitted in the passenger cabin of an aircraft. The checkpoint supervisor was required to be notified if an item in this category was encountered. Passengers would be given the option of having those items transported as checked baggage. “Mace,” “pepper spray,” as well as “tear gas” were categorized as hazardous materials and passengers could not take items in that category on an airplane without the express permission of the airline.

On the other hand, pocket utility knives (less than 4 inch blade) were allowed. The Checkpoint Operations Guide provided no further guidance on how to distinguish between “box cutters” and “pocket utility knives.”

One of the checkpoint supervisors working at Logan International Airport on September 11, 2001, recalled that as of that day, while box cutters were not permitted to pass

through the checkpoint without the removal of the blade, any knife with a blade of less than four inches was permitted to pass through security.

In practice, we believe the FAA's approach of admonishing air carriers to use common sense about what items should not be allowed on an aircraft, while also approving the air carrier's checkpoint operations guidelines that defined the industry's "common sense," in practice, created an environment where both parties could deny responsibility for making hard and most likely unpopular decisions.

*What happened at the checkpoints?* Of the checkpoints used to screen the passengers of Flights 11, 77, 93 and 175 on 9/11, only Washington Dulles International Airport had videotaping equipment in place. Therefore the most specific information that exists about the processing of the 9/11 hijackers is information about American Airlines Flight 77, which crashed into the Pentagon. The staff has also reviewed testing results for all the checkpoints in question, scores of interviews with checkpoint screeners and supervisors who might have processed the hijackers, and FAA and FBI evaluations of the available information. There is no reason to believe that the screening on 9/11 was fundamentally different at any of the relevant airports.

Return again to the perspective of the enemy. The plan required all of the hijackers to successfully board the assigned aircraft. If several of the hijackers failed to board, the operational plan might fall apart or their operational security might be breached. To have this kind of confidence, they had to develop a plan they felt would work anywhere they were screened, regardless of the quality of the screener. We believe they developed such a plan and practiced it in the months before the attacks, including in test flights, to be sure their tactics would work. In other words, we believe they did not count on a sloppy screener. All 19 hijackers were able to pass successfully through checkpoint screening to board their flights. They were 19 for 19. They counted on beating a weak system.

Turning to the specifics of Flight 77 checkpoint screening, at 7:18 a.m. Eastern Daylight Time on the morning of September 11, 2001, Majed Moqed and Khalid al Mihdhar entered one of the security screening checkpoints at Dulles International Airport. They placed their carry-on bags on the x-ray machine belt and proceeded through the first magnetometer. Both set off the alarm and were subsequently directed to a second magnetometer. While al Mihdhar did not alarm the second magnetometer and was permitted through the checkpoint, Moqed failed once more and was then subjected to a personal screening with a metal detection hand wand. He passed this inspection and then was permitted to pass through the checkpoint.

At 7:35 a.m. Hani Hanjour placed two carry-on bags on the x-ray belt in the Main Terminal checkpoint, and proceeded, without alarm, through the magnetometer. He picked up his carry-on bags and passed through the checkpoint. One minute later, Nawaf and Salem al Hazmi entered the same checkpoint. Salem al Hazmi successfully cleared the magnetometer and was permitted through the checkpoint. Nawaf al Hazmi set off the alarms for both the first and second magnetometers and was then hand-wanded before

being passed. In addition, his shoulder-strap carry-on bag was swiped by an explosive trace detector and then passed.

Our best working hypothesis is that a number of the hijackers were carrying permissible utility knives or pocket knives. One example of such a utility knife is this “Leatherman” item. We know that at least two knives like this were actually purchased by hijackers and have not been found in the belongings the hijackers left behind. The staff will pass this around. Please be careful. The blade is open. It locks into position. It is very sharp.

According to the guidelines on 9/11, if such a knife were discovered in the possession of an individual who alarmed either the walk-through metal detector or the hand wand, the item would be returned to the owner and permitted to be carried on the aircraft.

### **Onboard Security**

Once the hijackers were able to get through the checkpoints and board the plane, the last layer of defense was onboard security. That layer was comprised of two main components: the presence of law enforcement on the flights and the so-called “Common Strategy” for responding to in-flight security emergencies, including hijacking, devised by the Federal Aviation Administration in consultation with industry and law enforcement.

But on the day of September 11, 2001, after the hijackers boarded, they faced no significant security obstacles. The Federal Air Marshal Program was almost exclusively directed to international flights. Cockpit doors were not hardened. Gaining access to the cockpit was not a particularly difficult challenge.

Flight crews were trained not to attempt to thwart or fight the hijackers. The object was to get the plane to land safely. Crews were trained, in fact, to dissuade passengers from taking precipitous or “heroic” actions against hijackers. We will have more to say about the Common Strategy in the staff statement to come later today.

### **Conclusion**

From all of the evidence staff has reviewed to date, we have come to the conclusion that on September 11, 2001, would-be hijackers of domestic flights of U.S. civil aviation faced these challenges:

- avoiding prior notice by the U.S. intelligence and law enforcement communities;
- carrying items that could be used as weapons that were either permissible or not detectable by the screening systems in place; and
- understanding and taking advantage of the in-flight hijacking protocol of the Common Strategy.

A review of publicly available literature and/or the use of “test runs” would likely have improved the odds of achieving those tasks.

The 'no-fly' lists offered an opportunity to stop the hijackers, but the FAA had not been provided any of their names, even though two of them were already watchlisted in TIPOFF. The prescreening process was effectively irrelevant to them. The on-board security efforts, like the Federal Air Marshal program, had eroded to the vanishing point. So the hijackers really had to beat just one layer of security—the security checkpoint process.

Plotters who were determined, highly motivated individuals, who escaped notice on no-fly lists, who studied publicly available vulnerabilities of the aviation security system, who used items with a metal content less than a handgun and most likely permissible, and who knew to exploit training received by aircraft personnel to be non-confrontational were likely to be successful in hijacking a domestic U.S. aircraft.