Second public hearing of the National Commission on Terrorist Attacks Upon the United States

Statement of Major General O.K. Steele to the National Commission on Terrorist Attacks Upon the United States
May 23, 2003

Chairman Kean, Vice Chairman Hamilton, and distinguished members of the Commission: thank you for inviting me to this public hearing to share my views on our nations' civil aviation security system and what security improvements have and should be made in order to continue to strengthen that system. I am honored to be here to offer my personal perspective on this important issue.

Background. On 1 October 1990, I retired from the U.S. Marine Corps after 35 years of active military service. Two weeks later the Administrator of the FAA, Admiral James Busey, USN, (Ret) recommended me for the newly designated position of Assistant Administrator for Civil Aviation Security (ACS-1). Secretary Skinner of the Department of Transportation subsequently approved this recommendation and my appointment became effective on 1 November. Several weeks later on 16 November, President Bush signed Public Law 101-604, the Aviation Security Act of 1990, thereby strengthening significantly the role of the federal government in civil aviation security.

For the most part, the Aviation Security Act of 1990 was based on a majority of the findings and recommendations of the President's Commission on Aviation Security and Terrorism. Convening in November of 1989 under the able Chairmanship of Ann McLaughlin and using the Pan Am 103 tragedy as its principal point of reference, the Commission spent six months closely evaluating the existing aviation security system, options for handling terrorist threats and the treatment of families of victims of terrorists acts. By 15 May 1990, when the Commission finished its analysis and had submitted its' final report to the President, some 31 recommended actions had been directed at the FAA, 11at the Office of the Secretary of Transportation, 15 at the Department of State as well as a few others aimed at the intelligence community, namely the FBI and the CIA.

When I first read and reread the Commission's report in October of 1990, I considered it then to be one of the most comprehensive and useful governmental studies produced in this city. As I reflect on its worth and value today, I still look upon it as a model document. For me personally, it provided an unvarnished insight into the complexities and vulnerabilities of the national and international civil aviation system. It also gave me a profound appreciation for the scope of mutually supporting layers of security that are needed daily to protect civil aviation on a global scale, and most importantly, its passengers and crews against acts of terrorism as well as lesser threats of criminal interference. As mentioned previously, it was primarily this document, along with a number of Congressional hearings, which provided the bulk of the rationale for what later became the 1990 Aviation Security Act. As you are well aware, this Act mandated a host of regulatory responses, security program guidelines, establishment of new positions, Congressional reports, and other research and development and administrative initiatives. As I recall, the FAA Office of Civil Aviation Security (ACS), was responsible for completing some 38 separate actions, with specified deadlines for each, in order to come into full compliance with the Act.

Although I did not realize it initially, it wasn't long before I came to appreciate that the President's Commission Report, along with the ensuing Aviation Security Act of 1990, even with all of its short fused deadlines, was actually a blessing in disguise. First, the ACS organization for which I was now responsible had become badly demoralized by the Pan Am 103 tragedy and by the aftermath of almost two years of continuing investigations and inquiries into what had gone wrong and why the system failed. Now all the divergent views of most of the professionals in the business had been heard and carefully analyzed; conclusions had been reached and the debates pertaining how to proceed were over. Congress had spoken and the President had agreed. Fortunately, this enabled the ACS staff to stop dwelling on the failures of the past, and instead, start concentrating on the remedies needed for the future. Secondly, the President's Commission and the 1990 Act together, not only provided us with clear path to follow, but also the authority to implement its provisions with all deliberate speed. The campaign plan we formulated for carrying out this charge took full advantage of the momentum that had been handed to us.

AVIATION SECURITY HIGHLIGHTS 1990-1993

But implementing the Act was not the sole imperative pushing us to move quickly. In December the military build-up of coalition forces for "Desert Shield" was in full swing. Should the decision be to use force to liberate Kuwait, the risk of terrorist acts both overseas and in the U.S. would be high. With this in mind the ACS staff, in collaboration with representatives from the airlines and U.S. airports, drafted a contingency plan that called for extraordinary security procedures to be put in place immediately throughout the entire civil aviation system, in the event hostilities broke out. We also developed a scheme to triple the presence of ACS security inspectors to those overseas airports we regarded as being in the 'high risk' category. Thus when Admiral Busey called me into his office on that January morning to inform me confidentially that the B-52s were taking off from Barksdale AFB, the additional security measures for airlines and airports were in effect before the first bomb had hit Iraq. These measures stayed in place until they were gradually relaxed starting in April.

When I was appointed as ACS-1, the intelligence community was unanimous in its view that national and transnational terrorist groups, operating mainly overseas in the Middle East, Europe, Africa and in Asia posed the greatest threat to our civil aviation network, particularly for U.S air carriers that routinely flew to these regions. By this time the weapon of choice for a number of these terror groups had shifted from hijackings, to blowing up planes in flight using improvised explosive devices (IEDs) brought aboard the aircraft through checked baggage. Indeed, this had been the method used in the catastrophic loss of Pan Am Flight 103. Therefore, many of the provisions of the 1990 Act required ACS to put more stringent security measures in place and to evaluate all the new technologies that might more effectively detect the growing IED threat.

Listed below are five themes that cover the elements of the 1990 Act and a brief summary of some, but not all of the actions taken to implement them:

Organization and Personnel: Both the Office of Secretary and the FAA created specialized organizations to handle aviation security. Both were headed by Senior Executives who reported directly to the Secretary or the Administrator. Eighteen Civil Aviation Security Liaison Officers (CASLO) were placed overseas to cover foreign airports. Nineteen Federal Security Managers

were established and stationed in the nations' largest and busiest airports (Category X) reporting directly to ACS-1. New rules were published that established employment standards, provided for employment investigations and criminal history background checks and raised the performance/training standards for airport and air carrier security personnel. ACS recruited, joined and trained over two hundred new aviation security inspectors/agents to meet the expanding requirements directed by the law.

Research, Engineering and Development: We increased the intensity of explosive and weapons detection and air container hardening programs and expanded the scope of work, particularly developing a comprehensive human factors program. An R, E&D Scientific Advisory Panel of independent experts was established to critically examine our programs and provide advice to the ACS staff.

Explosive Detection Systems (EDS): The final performance criteria for automated bulk explosives detection systems and the certification test plan with independently developed test protocols were published in 1993; this was after the assigned deadline but the protocols did meet the requirements for testing mandated by the law. (The first EDS, the INVision CTX-5000, was certified in December 1994 and was operationally tested in three airports in accordance with the ACT.)

Intelligence and Threat Assessment: Guidelines were developed and published for airline employees on reporting threats, for public notification of threats and for threat notification of flight and cabin crews. Cooperation and coordination between the ACS Office of Intelligence (ACI) and the FBI and CIA improved greatly. ACI placed full time liaison officers at the FBI, CIA, DOS headquarters and ACS-1 became a member of the counter-terrorism sub committee of the NSC.

Technical Airport and Air Carrier Security Issues: A review and revalidation for foreign air carrier security programs to determine whether or not they provided a similar level of protection was completed. Joint FAA/FBI threat and vulnerability of all Category X airports was completed and comprehensive security plans were drawn up for each of these major airports. Cargo and mail security procedures were tightened significantly and guidelines were published on incorporating good security practices for contractors involved in future airport construction or renovation.

In addition to meeting all the provisions of the Act, it also became clear to me as I visited the various ACS field offices around the country that three of the 18 separate programs for which I was responsible, were in poor shape and needed shoring up. One was the Canine Program, the second Hazardous Materials, and the third was the Federal Air Marshal Program (FAM). Putting the first two back on track was done with relative ease. Overhauling the FAM Program took much longer to achieve. However, by bringing in a fresh leadership team that established higher physical fitness standards, insisted on running team drills under realistic tactical scenarios, and by raising the FAM shooting qualification skills to the same level used by Special Operations Forces, gradually full confidence in our FAM teams was restored. Because only a limited number of our agents were qualified as FAMs, we only deployed the teams on overseas "high risk routes," as determined by our intelligence analysts. Our goal was to have at least one team on a mission at all times. Because their presence on a scheduled flight is unpredictable, FAMs in my opinion, provide a worthwhile deterrent against hijacking.

ATTEMPTS TO MEASURE EFFECTIVENESS: Is our aviation security system better than, less than, or about the same as it was yesterday? While I was ACS-1 I don't believe a day went by that our security specialists, their field supervisors and we in the ACS headquarters did not ask ourselves that question. Answering it was not always easy. There were days that suggested progress was indeed being made and that the ball was moving steadily toward the mid-field stripe; on other days, we might come to work and suddenly find that we were back defending our own goal line again.

For most of the traveling public, their concept and knowledge of civil aviation security is limited to what they see and experience as they pass themselves and their carry-on luggage through the air terminal passenger-screening checkpoint. While the screening checkpoint may be the most visible feature and serve as a vital last line of defense, few realize that it actually represents only about 15 per cent of the total aviation security network. What is less known is the security measures that are taking place in the baggage make-up areas on the lower level. Nor are many people aware of all the access controls stations that lead to the Airport Operating Area (AOA) and that in this country, over 750,000 people must have criminal background investigations conducted in order to receive their special airport identity badges so that they can perform their daily jobs of refueling aircraft, cleaning the cabins, delivering in-flight meals, or delivering the U.S. Mail and cargo. Meanwhile, all of this activity is being constantly monitored from some large control station through unseen security cameras. No wonder when one examines closely all the potential threat vectors that require some level of protection or security control at an airport today, the complexities of the problem can truly become mind-boggling. Furthermore, after awhile I began to better understand and appreciate that, as we believe there is an "aviation security system" we must also conclude that we are only as strong as our weakest gateway. Thus Fargo can be as critical as JFK.

But the nexus of this question of how good or how bad is security, usually boiled down to the one critical link-people; the human factor if you will-not machines. For example, during the first gulf war, achieving high standards of security and maintaining them was not difficult. People on both sides of the security screen had good situational awareness and understood the need to stay alert and vigilant. By the same token, once the threat begins to fade, or is perceived to have gone away altogether, then complacency invariably creeps in and the need to continue those same good security practices seems less of an imperative. This need for constancy by everyone who is employed within the system was brought home to me during my last few months as ACS-1. The Inspector General of the Department of Transportation sent out inspector teams to evaluate access control points at five domestic airports. To my deep chagrin and embarrassment the reports that came back were dismal. In many instances the inspectors were able to pass through the security control point as if they were non-existent, principally by piggybacking behind a cardholder who paid no attention to them. Nor did airline personnel in the ramp area always challenge the inspectors for not wearing a security badge once they were inside. Despite the painful report, my staff and I did appreciate learning that serious gaps had sprung up in the system again and the need for repair was urgent. We were back at our own ten-yard line again.

Of course our field offices and security specialists were out constantly assessing the security of airports in their respective

regions and conducting tests of passenger security checkpoints. The Intelligence and Operations Directorates would also publish reports giving statistical data on such things as: the number of bomb threats directed against U.S. airports and airlines, the number of weapons detected and confiscated at checkpoints (2700-2800 per annum) number of enforcement cases applied against an airline or airport and test object detection rates at screening points, to name just a few. These measurements were useful in determining trends, or making comparisons between different regions, but never adequately told us where the "holes" were in the system. For example, in the early 1990's the test objects introduced by our agents at a passenger screening point to evaluate screener competence were far too basic and woefully out of date to be challenging. Nor did they begin to replicate the serious threats that artful terror bombers were capable of making. Consequently, the 92 percent detection rate figures were of little comfort when we knew that results from our new trial modules were significantly lower.

By the end of the first year on the job, I found that one the best tools I had at my evaluation kit, was what we referred to as the Red Team. Using SEALS, the U.S. Navy had been employing Red Teams to test security of their naval installations for years. Consequently, it was Admiral Busey's concept to create an internal Red Team under ACS-1. Its purpose was to truly test the integrity of the security system by going out unannounced and covertly try to breach our defenses using all the guile and cunning of our adversaries. One of our intelligent specialists from ACI with over 22 years of counter-intelligence experience with the U.S. Air Force was appointed to head the team. It took almost a year to hire and train eight to ten men and women for the team, all of who came from similar backgrounds of military intelligence of one branch of service or another. This was not cowboy stuff. Strict protocols were written and monitored to keep what the team could do and not do and it was kept under tight control. Air Line Security Directors were notified that such a group had been formed, but were never told where or when they might be testing a security checkpoint or a required procedure. Likewise, ACS field managers also never knew beforehand if a Red Team was operating within their regions. Serious successful breaches to the system were reported to me, or my Deputy immediately.

Once the Red Team was trained and ready, the first task assigned to it was to test passenger-baggage match (PBM) procedures of all U.S. air carriers flying in and out of various airports in Europe. You'll recall that it was Pan Am's failure to properly carry out this procedure that caused the loss of Flight 103. For a solid week the team, traveling alone or in twos from different directions on different U.S. airlines tried to introduce their bags onto either an originating or a connecting flight and then would purposely miss the last call for boarding. The object was to determine if the bag was in fact pulled from the aircraft before departure in accordance with the PBM procedure and the international standard. When the team returned to Washington D.C., I was relieved to learn that not one bag had gotten through. That type of information told me a lot. We repeated the process in the Pacific and the Far East with the same results. Following that series of tests, we then directed the team's efforts to evaluating various security checkpoints while quietly introducing the new test modules. Their mission included sampling a number of domestic checkpoints at different sized airports and objectively determine which were the strongest, which were the weakest and why was this so. Again the answer came back, it was people. Invariably, the checkpoint seemed to be as strong or as weak the supervisor (CSS) who was running it.

During my final months as ACS-1 my staff and I began to reassess where we were and whether the campaign plan we had formulated earlier needed course corrections. Certainly the situation and the environment we were working in had changed from three years ago. To a degree, we had fallen victim success and we were losing the steam and momentum we once had. There had been no serious mishaps or breaches into the "system" and thus security was once again taking a back seat to other more pressing concerns. Even my own agency had earlier cut the 120 new ACS positions that had been planned for that year. Moreover, the depressed state that the airline industry was in had stiffened their resistance to making new security investments. Although we anticipated EDS would be ready for deployment within the next three years, Airline CEOs were already making sending signals that those systems would have to be purchased by the government.

We still saw the highest threat as being overseas. Therefore, there could be no reductions in either the number of agents we had stationed abroad, nor any lessening to the extraordinary security measures we had in place there. To complicate matters, recent figures we had received on both hijackings and bombings did suggest that airports and airliners had indeed been hardened, yet at the same time we were already beginning to see signs of an emerging threat from shoulder fired missiles. From these assessments ACS adopted a strategy of flexible response based on these principles: (1) maintaining a defense in depth (deter-delay-defend) without relying totally on any single procedure or technology. (2) Economy of Force- consolidate and improve the gains that had been made, adopt it as the new minimum base line level for the domestic system, and be ready to rapidly reestablish our Gulf War contingency plans, to include requiring point-to-point Passenger Bag Matching if the need arises (3) Concentrate our resources at known danger points. Example: push automated training programs such as Safe Passage and SPEARs to raise the level of performance and detection at passenger screening checkpoints; encourage airline investments into the Computer Assisted Profiling System (CAPS).

My successor as ACS-1 was retired Admiral Cathal Flynn, U. S. Navy. In the spring of 1995 the security measures contained in previously agreed contingency plans went back into effect and essentially remained in place as the domestic aviation security base line until 2001.

RECOMMENDED CONSIDERATIONS FOR THE FUTURE

Threats. I believe the major threats we face today and for the next few years will be: one, IEDs in checked baggage; the second is car bombs detonated as close to a terminal as possible; third, a coordinated terror campaign against cargo flights using smaller bombs; fourth, shoulder-launched missiles.

The most effective way to counter the first threat is to deploy EDS to all airports, including the smaller ones where right now trace detection is being used as a stopgap measure. As new EDS equipment comes on line, there also needs to be a parallel operator-training pipeline that instructs the TAS screeners to do "on screen resolutions" in order to exploit the full capabilities of this equipment. Blast-resistant containers for both cargo and baggage have been under test and development by the Department of Transportation since 1991 and are now being evaluated under flight operations. This program could also significantly reduce the primary and tertiary threat and thus should be given high priority.

The most visible and therefore one of the most critical issues confronting TSA today is the security checkpoint. The problem appears to me to be both technical and human factors. The basic weakness of x-ray equipment remains; it does not provide adequate probability of detection (PD) for identifying explosives or other bomb components. This means delays in the line until a supervisor can resolve questionable presentations. Ultimately, computed tomography should be deployed to all screening checkpoints to provide the optimum PD for IEDs and also give screeners a high quality image for the identification of test or threat objects. On the human side, the need for more technical training for the operators is clearly evident. I understand that in this regard good progress is being made in units that are TIP capable. Formal leadership training for the checkpoint supervisors is a must. Also, the Federal Security Directors need to step up to the plate and negotiate with the airport authorities for better conditions for the TSA staff, such as break rooms etc.

I am a big fan of EOD personnel. They are like combat engineers in a combat - you can't have enough of them. I would think that it would be in the interest of TSA to have an EOD presence at all the airports above the Category 2 level. With 20-year retirements, I suspect there are many military EOD and police bomb technicians who would be interested in a second career resolving screening alarms and handling unattended bags. When not resolving alarms they could be used as instructors during on-the-job local training sessions.

It is unclear to me how the TSA is measuring the effectiveness of the aviation security system today. By that I mean not just screening checkpoints, but the integrity of the entire system. The Congress and the American people have seen a lot of people and tax dollars being thrown into fixing this problem. The day is coming when they will be asking for an accounting. Is the system better than it was a year ago? If so, how much better and are the costs justified; can this be defended with solid analytical data? Will performance based evaluations such as TIPs be used to evaluate screener proficiency?

I strongly believe that having a sizable Red Team within TSA capable of conducting unannounced covert evaluations on the security of not only aviation, but also all modes of transportations, has merit. Red Teams keep our guardians on their toes, reduces complacency and provides the leadership with the knowledge of where truth lies. Such a concept is not only authorized but is encouraged under the law. See 49 U.S. Code, Chapter 44916 "---shall conduct periodic and unannounced security assessments."

From what I can glean from the newspapers, the Federal Security Directors desperately need formal training.

Computer Assisted Profiling System (CAPS) is in my view useful and worth the investment. Its purpose is to identify the "knowns" and when the peaks put a strain on the screening process, it allows you so spend more time to concentrate on the "unknowns." Simply put, it is a winnowing process. The million-miler is not the terrorist. Conversely however, it is not, nor should it be a means to find a terrorist. I am not aware of any method of finding terrorists in an airport environment that has thus far proved to be effective or efficient. Nor am I a fan of the so called Israeli profiling method of standing eyeball to eyeball asking intrusive questions of passengers that in our society we have no right to ask.

I am among those who is not alarmed by the arming of pilots. Even if less than 50 percent of the pilots choose to do so, it

creates unpredictability for the hijackers. Are they or aren't they? They must now ask themselves. However, once there is a requirement to reinforce the entire bulkhead separating the cockpit from the cabin and not just the door, and where necessary the floor such as in the 747, perhaps then the need will go away and the policy should be reevaluated.

Finally Mr. Chairman, let me say that I am confident that the day is coming when the United States will have a very robust aviation security system that is capable of defending us against the threats we face today. However as we move toward achieving that goal, we must ensure that a similar and parallel program using the latest EDS and trace equipment is also being installed overseas. Otherwise, all we will have done is cause the terrorist to shift their operations to some other location and where our people will still be at risk.

I thank you for your time and am happy to respond to any question the Commission may have.