For Release on Delivery
Expected at
2:00 p.m. EDT
Thursday
May 22, 2003
CC-2003-117

Statement Before the National Commission on Terrorist Attacks Upon the United States on Aviation Security

Statement of
The Honorable Kenneth M. Mead
Inspector General
U.S. Department of Transportation

Chairman Kean, Vice Chairman Hamilton, and Members of the Commission:

We appreciate the opportunity to testify. The principal focus of our testimony is the state of aviation security prior to September 11th, actions taken to improve aviation security since that tragic day, and areas that still require attention. Our testimony is based on audits and criminal investigative work spanning a number of years covering a broad range of subjects—airline use of explosives detection systems, security technologies, passenger and baggage screening, airport access controls, and cargo security. Following the horror of the September 11th attacks, we testified several times on these same subjects and, in doing so, highlighted weaknesses in both the design and execution of the aviation security system in place before September 11th. We believe aviation security will require continuous improvement and vigilance.

As you know, the Federal Aviation Administration (FAA) had responsibility for overseeing the security of the Nation's aviation system prior to and immediately following September 11th. That responsibility transferred to the Transportation Security Administration (TSA) upon enactment of the Aviation and Transportation Security Act (Act) in November 2001. As part of the largest reorganization of Government since World War II, TSA, along with 21 other agencies, was transferred to the Department of Homeland Security (DHS) on March 1, 2003.

It is important to note that aviation security is noticeably and demonstrably much tighter now than before September 11th. During the 16 months after the passage of the Act, at the direction and under the leadership of Secretary Mineta and the Department of Transportation (DOT), much was accomplished to improve aviation security. The aviation security system in place before September 11th had undergone some incremental improvements over the years, such as deployment of explosives detection machines, and probably provided a deterrent value to certain types of threats. However, neither the system nor the model on which it was based worked very well, and there were significant weaknesses in the protection it provided—even for the type of threat the model was designed to prevent. As a result, this model has undergone fundamental change.

Before September 11th, the aviation security model was mostly based on reacting to known security threats instead of being proactive against potential threats. The model, dating back to the early 1970's, was implemented through a system of shared responsibilities. Industry provided and paid for the security; FAA's role was to establish security requirements and ensure compliance with these requirements.

Within the model were counter pressures to control security costs and limit the impact of security on aviation operations, so that industry could concentrate on its

primary mission of moving passengers seamlessly and safely through the system. In our opinion, these counter pressures manifested themselves as significant weaknesses in the security system that we and others repeatedly found during audits and investigative work. Many of these weaknesses, even for the threats the model was designed to prevent, existed for years, such as underutilization of bulk explosives detection machines, lack of performance standards for screening companies and their employees, inadequate controls to prevent unauthorized access to secure areas of the airport, ineffective background investigation requirements for employees working at the airport, and deficiencies in the cargo security program. For example:

- Air carriers were required to screen passengers and their carry-on baggage but would typically award the screening contract to the lowest bidder. Employees of these screening companies typically received only the minimum required security training (15 hours) and usually received prevailing minimum wages—it was not unusual for the starting wages at airport fast-food restaurants to be higher than the wages screeners received. These conditions, along with others, resulted in screener turnover rates as high as 400 percent annually.

  Our 1996 report on efforts to improve airport security, and audits going back nearly a decade before this, found that screeners frequently failed to detect threat items—firearms and mock explosives—at security checkpoints. However, FAA never issued a final rule on the certification of screening companies to address the deficiencies in screening operations, even though the rule was required by the Federal Aviation Reauthorization Act of 1996. In early 1997, FAA issued an Advanced Notice of Proposed Rulemaking (ANPRM) on certification of screening companies. It was withdrawn in May 1998 and re-issued in January 2000. FAA was prepared to issue its final rule on the certification of screening companies the week of September 10, 2001.

- In 1998, we found that air carriers were significantly underutilizing explosives detection systems (EDS) already deployed and that continued low use would affect operator proficiency and prevent effective measurement of how dependable the equipment was in actual operations. Overriding reasons that EDS was underutilized were that air carriers were only required to use the machines to screen the baggage of passengers selected by Computer-Assisted Passenger Prescreening System (CAPPS)[1] and the machine had a high false alarm rate. The requirement to screen only selectees' bags addressed the air

[1] CAPPS is an automated passenger prescreening system that uses information in airline reservation systems to separate passengers into a very large majority who present no security risk, and a small minority (known as selectees) who merit additional attention, such as having their checked baggage screened using explosives detection systems.

carriers' concerns that screening more than selectees' checked baggage would compound the delays air carriers were already experiencing in their operations. Therefore, equipment with a demonstrated ability to improve airport security often sat idle in airport lobbies.

- Criminal investigations we conducted before and after September 11th showed serious weaknesses in background checks of contract screener and airport workers. In October 2000, one of the Nation's largest private security companies pled guilty and paid more than $1 million in fines and restitutions for falsifying criminal history checks and screener qualification records at one of the Nation's largest airports. Before September 11th, little public attention was given to the seriousness of this issue.

  After September 11th, we participated in law enforcement sweeps at more than 30 airports nationwide. The sweeps resulted in the indictment or arrest of more than 1,000 individuals who had falsified records about their identities, criminal histories, or immigration status and, as a result, obtained airport identification badges that allowed access to secure areas of the airport.

- For years, air carriers resisted implementing positive passenger bag match (PPBM) on domestic flights, stating that it would be too costly and bring the aviation system to a standstill. Yet after September 11th, when air carriers were given the option of implementing PPBM or other security procedures until sufficient EDS were installed, air carriers chose PPBM as the preferred option and the system was not brought to a halt.

After September 11th, the model was fundamentally changed by moving much of the responsibility and cost for aviation security to the Federal Government. TSA and the DOT moved forward in standing-up an entirely new organization. Most noteworthy, TSA met the challenge to hire and train a federalized workforce to screen all passengers and their carry-on baggage by November 19, 2002, and, for the most part, to deploy the necessary equipment and federalized workforce to meet the December 31, 2002 deadline to screen all checked baggage. This required hiring and training a screener workforce of more than 60,000.

At the same time, TSA significantly expanded the Federal Air Marshals program with more flights being guarded now than at any time in history, and air carriers have strengthened cockpit doors. Also, more emphasis is being focused on gathering, coordinating, and disseminating intelligence on homeland and transportation security threats.

The new security model is much more likely to ensure strong aviation security than its predecessor. It is based on powerful lessons learned. However, a

cautionary note is in order. The sense of vigilance for and priority attached to tight security can dissipate with the passage of time from a terrorist event; this, in turn, may lead to a sense of complacency as well as pressures to relax security. To guard against this and ensure continuous improvement, we believe emphasis on the following will be of utmost importance: gathering intelligence information on homeland and transportation security; integrating EDS into baggage handling systems at the largest airports; investing in research and development for more effective equipment for screening passengers, their baggage, and cargo; implementing an aggressive covert testing program to evaluate operational effectiveness of security systems and equipment; establishing screener performance standards; and improving cargo security.

The foregoing must be accomplished in an environment that is cognizant of the need to build tight security into the aviation system in a manner that allows for the safe and efficient movement of aircraft and passengers. This is certain to be a continuous challenge for both TSA and the aviation community.

The Aviation Security Model in Place Before September 11th Was a System Geared Toward Reacting to Known Threats

Aviation security requirements were predicated largely on responding to threats that had been experienced or thwarted and often were put in place contemporaneously with or following a cycle of congressional or commission hearings. For example:

- S*creening checkpoint security* came about as a direct result of a series of aircraft hijackings worldwide during the late 1960's and early 1970's. In the 1970's, the model was designed around a set of rules to prevent aircraft hijackings. In nearly all cases, firearms were the weapons of choice for hijacking the plane. FAA adopted policies requiring the use of metal detectors for screening all passengers and x-ray machines for screening the passengers' carry-on baggage.

- *Airport access controls* were further strengthened after the crash of Pacific Southwest Airlines Flight 1771 in 1987, where a PSA employee smuggled a firearm onboard the flight and fatally shot his supervisor, the pilot and copilot, causing the plane to crash. The crash investigation found that the PSA employee, who had been put on unpaid leave pending a theft investigation, purchased a ticket for the flight and used his airline employee credentials to bypass security. FAA adopted policy to require that all members of any airline flight crew be subjected to the same security measures as the passengers.

- *Checked baggage security* was strengthened during the 1990's, after the bombing of Pan Am Flight 103 over Lockerbie, Scotland, in December 1988, and a subsequent unsuccessful terrorist plot in 1995 involving U.S. carriers' outbound flights from the Philippines. Following the bombing of the Pan Am flight, FAA embarked on the development of equipment to screen checked baggage for explosives.

The security threats underlying the model and the assumptions on which that model was based did not envision a scenario of commercial airliners being used as a weapon, or the use of "box cutters" by individuals who were prepared to die in the commission of their terrorist acts.

Within the Model There Were Counter Pressures to Control Security Costs and Limit the Impact of Aviation Operations

FAA's role did not include the direct provision of security; instead, FAA's role was to set guidelines; establish rules, regulations, policies and procedures; oversee and enforce industry's compliance with security requirements; and make judgments on how to meet threats to aviation based on information from the intelligence community. Air carriers were responsible for screening baggage, passengers, and cargo, including hiring private screening companies and deciding whether to actively participate in the deployment of EDS. Airport operators were responsible for the airport perimeter and facility security, operating and maintaining airport access control systems, and issuing airport identification.

Within this model, there were counter pressures to control security costs and limit the impact of security on aviation operations, so that industry could concentrate on its primary mission of moving passengers seamlessly and safely through the system. These counter pressures manifested themselves as weaknesses in the security system that we repeatedly found during our audits and investigative work—even for the threats the model was designed to prevent. Many of these weaknesses existed for years without permanent corrective actions. The following are areas we noted during our audits and investigative work prior to September 11th as needing immediate corrective action.

Security of Checked Baggage

EDS machines were developed to assist screeners in identifying threat items in passengers' checked baggage. In our 1998 report on Deployment of Explosives Detection Equipment, we recommended that FAA develop a strategy to more effectively utilize the EDS machines and enhance screener performance. Overriding reasons that EDS was underutilized were that air carriers were only required to use the machines to screen the baggage of passengers selected by

CAPPS and the machine had a high false alarm rate. The requirement to screen only selectees' bags addressed the air carriers' concerns that screening more than selectees' checked baggage would compound the delays air carriers were already experiencing in their operations. Therefore, equipment with a demonstrated ability to improve aviation security often sat idle in airport lobbies.

Congress passed the Aviation Security Improvement Act of 2000, which directed FAA to maximize the use of explosives detection equipment. However, FAA and TSA never utilized deployed EDS machines to the maximum extent possible until the December 31, 2002 deadline. These machines cost about $1 million each plus installation costs ranging from $300,000 to over $1 million. While the machines are capable of screening 125 *bags an hour*, we routinely found the vast majority were screening between 250 and 750 *bags per day*.

After numerous testimonies and reports, FAA took some action to increase utilization of bulk explosives detection machines. However, the utilization goals that FAA chose were too low. Bulk explosives detection machines in use have an immediate, powerful, and visible deterrent effect on potential terrorist attacks. One sitting idle does not.

Today, the operational landscape has changed, and what we found in the past—EDS machines sitting idle when plenty of bags were available for screening—is no longer the case.

Screening Checkpoint Security

Screening checkpoint operations have a long-standing history of system ineffectiveness going back as far as 1987 when General Accounting Office (GAO) investigators were able to successfully pass test weapons through screening checkpoints. Air carriers were required to screen passengers and their carry-on baggage, but would typically award the screening contract to the lowest bidder. Employees of these screening companies typically received only the minimum required security training (15 hours) and usually received prevailing minimum wages—it was not unusual for the starting wages at airport fast-food restaurants to be higher than the wages screeners received.

In our 1996 report on efforts to improve airport security, we found that screeners frequently failed to detect threat items at security checkpoints. In a 2000 report,[2] GAO found that long-standing problems combined to reduce screeners' effectiveness in detecting dangerous objects. The most notable were (1) rapid

[2] Aviation Security: Long-Standing Problems Impair Airport Screeners' Performance, Report Number GAO/RCED-00-75, dated June 2000.

turnover of screener personnel (as high as 400 percent annually), and (2) human factors issues—repetitive tasks and the need for adequate training—that for years affected screeners' hiring, training, and working environment. GAO found that, despite several laws enacted by Congress, concerns remained over screeners' ability to detect dangerous objects. Furthermore, FAA acknowledged that screeners' detection of dangerous objects during testing was unsatisfactory and was in need of improvement.

The Federal Aviation Reauthorization Act of 1996 directed FAA to certify screening companies and improve screener performance. In early 1997, FAA issued an Advanced Notice of Proposed Rulemaking (ANPRM) on certification of screening companies; it was withdrawn in May 1998 and re-issued in January 2000. FAA was prepared to issue its final rule on the certification of screening companies the week of September 10, 2001. However, following the September 11th tragedy, the DOT elected to delay publication of the final rule so that the Rapid Response Teams could re-evaluate the certification requirements.

Threat image projection (TIP) was an important component of FAA's final rule on certification of screening companies. TIP is a software program installed on x-ray machines being deployed at screening checkpoints at airports nationwide. TIP exposes screeners to projected simulated threats on a regular basis to train them to become more adept at detecting threats and to enhance their vigilance. In its final rule, FAA planned to require that TIP be used to measure the performance of individual screeners and screening companies. However, FAA never established standards for measuring screener performance based on a combination of TIP testing and actual field testing by FAA.

The Act required that TSA have in place a federalized workforce to screen all passengers and their carry-on baggage by November 19, 2002. TSA implemented standards for selecting and training its screener workforce, and is formalizing an annual re-certification program for existing screeners. A prototype program is scheduled to begin in June 2003.

Airport Access Controls

Controlling access to secure areas[3] of the airport is critical in protecting the airport's infrastructure and aircraft from unauthorized individuals. During late 1998 and early 1999, we successfully accessed secure areas in 68 percent of our tests at eight major U.S. airports. Once we entered secure areas, we boarded

[3] OIG uses the term **secure area** to define the area of an airport where each person is required to display airport-approved identification. Each airport defines this area, which may be the entire Air Operations Area or may be limited to a smaller, more restrictive area.

aircraft 117 times. The majority of our aircraft boardings would not have occurred if employees had taken the prescribed steps, such as making sure doors closed behind them.

In addition to recommending that FAA work with airport operators and air carriers to implement and strengthen existing controls to eliminate access control weaknesses, we also recommended that comprehensive training programs be developed that teach employees their role in airport security, and that airport operators and air carriers make employees accountable for compliance. These recommendations along with others were incorporated into the Airport Security Improvement Act of 2000.

Conducting Background Investigations and Criminal History Checks

Our 2000 report on Controls Over Airport Identification Media[4] looked at industry's compliance with FAA's background investigation requirements at six U.S. airports; we found that the requirements were ineffective, and that airport operators, air carriers and airport users[5] frequently did not comply with these requirements.

Criminal investigations we conducted before September 11th also showed serious weaknesses in industry's compliance with background investigations and criminal history checks. In October 2000, one of the Nation's largest private security companies pled guilty and paid more than $1 million in fines and restitutions for falsifying criminal history checks and screener qualification records at one of the Nation's largest airports.

We made recommendations to FAA to strengthen background investigation requirements to include initial and randomly recurring Federal Bureau of Investigation (FBI) criminal checks for all employees; expand the list of crimes that disqualify an individual from unescorted access to secure airport areas; and incorporate in background investigation requirements the use of credit checks and drug tests to help assess whether individuals can be trusted with the public's safety and be permitted to work in secure airport areas.

The Airport Security Improvement Act of 2000 incorporated some of our recommendations and required FBI criminal checks at the Nation's largest airports as of December 2000. However, other airports were not scheduled to enter this program until December 2003, even though FAA had stated the capacity to

[4] Report on Controls Over Airport Identification Media (Report Number AV-2001-010, December 7, 2000).

[5] Airport users include foreign air carriers, non-air-carrier airport tenants, and companies that do not have offices at the airport, but require access to the secure airport areas.

process additional checks exists. We recommended that all airports be required, immediately, to conduct criminal checks for all employees that have access to secure airport areas, and for all screeners, including cargo screeners. Also, criminal checks must not be restricted to first-time applicants, as the current law provides, but should include all employees regardless of their employment date. Further, criminal checks must be recurring.

Airport sweeps of illegal activities involving fraudulently obtained airport identification have demonstrated the need to conduct both a background investigation and a criminal history check before issuing airport identification. After September 11th, we participated in law enforcement sweeps at more than 30 airports nationwide. The sweeps resulted in the indictment or arrest of more than 1,000 individuals who had falsified records about their identities, criminal histories, or immigration status and, as a result, obtained airport identification badges that allowed access to secure areas of the airport.

Cargo Security

FAA's Cargo Security Program was intended to address security risks and prevent terrorist attacks on commercial passenger aircraft through air cargo. The Program was guided by a primary principle—the terrorist does not want to be identified. Unfortunately, the events of September 11th illustrated that this one principle can no longer be relied on to deter terrorists who are willing to be identified and die in the course of carrying out their mission. Therefore, new principles must be added to better ensure the safety of the public.

In 1997, we advised FAA of the need to strengthen its approval procedures for indirect air carriers[6] and ensure compliance with cargo security requirements. In September 2001, we briefed FAA on the results of our follow-up audit of FAA's Cargo Security Program. FAA has taken action to strengthen the program since September 11th by no longer allowing air carriers to accept cargo from unknown shippers and strengthening the requirements for becoming a known shipper—an entity with an established shipping history. However, FAA did not take actions to strengthen procedures for approving indirect air carriers to ship cargo on passenger aircraft, and weaknesses continue in this area.

After September 11th, FAA took steps to strengthen cargo security, including issuing security directives and an emergency amendment that prohibit air carriers from accepting cargo from unknown shippers, and establishing additional requirements for classifying shippers as "known." However, the Program

[6] An indirect air carrier is any person or entity, excluding an air carrier that engages indirectly in the transportation of property by air, and uses the services of a passenger air carrier, such as a freight forwarder. This does not include the U.S. Postal Service.

continues to rely on the known shipper policy. The Aviation and Transportation Security Act requires the screening of all cargo but did not set an implementation date, and only a limited amount of cargo is currently screened. Cargo security continues to receive close attention from Members of Congress, with several bills being introduced to improve aviation cargo security.

Covert Testing

Industry's implementation of established security requirements also left considerable room for improvement; and FAA's oversight, enforcement, and regulation-issuing activities were often ineffectual in achieving permanent improvement. We investigated allegations, brought by a former member of FAA's "Red Team," that covert testing results were deliberately covered up by FAA's Office of Civil Aviation Security. The Red Team was a small, special FAA Headquarters-based unit formed after the bombing of Pan Am Flight 103. Its primary mission was to conduct covert testing of airport security operations worldwide.

This covert testing was distinguished from FAA's routine regulatory compliance testing carried out by local FAA security field offices. Testing conducted by the local field offices was subject to standardized FAA protocols that in our opinion, were not comprehensive or realistic. For example, a typical test for a screener would include a firearm or fake bomb placed inside a carry-on bag with little, if any, clutter. The Red Team's testing was a more rigorous and creative "out of the box" approach to testing. The Red Team's techniques were similar to those we employed in conducting our covert testing.

While we did not substantiate that any deliberate cover-up occurred, we found that FAA's Red Team program suffered from inadequate agency follow-up action to Red Team testing, despite consistently poor test results over time and the lack of sustained improvement in security. We also found that once Red Team results were forwarded to air carriers and shared with FAA field elements, there was no follow-up communicated to the Red Team about any corrective actions resulting from their tests. Based on our findings, we recommended that TSA incorporate a number of key provisions in its successor program to FAA's Red Team. Doing so would translate the findings of TSA's covert testing program, in a well-managed manner, to substantive enhancements in key areas such as screener training, screener performance/accountability measures, technology applications, and local testing performed by TSA's field regulatory element.

In November 2001, President Bush, Secretary Mineta, and Deputy Secretary Jackson directed the Department of Transportation's Office of Inspector General to conduct undercover audits of security performance at airports nationwide, to

evaluate the industry's compliance with the then FAA security requirements. We found areas with very high levels of compliance such as passenger prescreening, the screening of selectee checked baggage, and not accepting small packages from unknown shippers. However, despite the additional requirements mandated by FAA following September 11th, there were areas where severe lapses in security occurred, including screening of passengers and their carry-on bags at screening checkpoints.

The New Security Model Is Not an End State and Requires Continuous Improvement

The new security model is much more likely to ensure strong aviation security than its predecessor. It is based on powerful lessons learned. However, a cautionary note is in order. The sense of vigilance for and priority attached to tight security can dissipate with the passage of time from a terrorist event; this, in turn, may lead to a sense of complacency as well as pressures to relax security. To guard against this and ensure continuous improvement, we believe emphasis on the following will be of utmost importance.

Remain Proactive. More emphasis is being focused on gathering intelligence on homeland and transportation security threats, and we have better coordination among intelligence agencies. Those responsible for protecting the Nation's transportation systems must address potential threats as opposed to simply reacting to known threats. In doing so, they must also ensure the flow of information from the intelligence community beyond aviation to the surface transportation and maritime sectors. TSA is extending its focus to these other sectors.

Move Forward on EDS Integration. TSA needs to move forward with integrating EDS into baggage handling systems at the largest airports. Some estimates put the cost of integrating the equipment upwards of $3 billion. For example, at Boston Logan International Airport, integrating EDS into its baggage handling system cost around $146 million. The ultimate cost of integrating EDS at the largest airports will depend on the type of structural changes required in the baggage make-up area, and the efficiency and reliability of the equipment. At this point, it is unclear how long this integration will take, how much it will cost, and who will have to pay for it. However, this integration is necessary to improve the efficiency and effectiveness of the security system.

Strengthen Research and Development. It is clear that integrating EDS into the baggage systems at the largest airports will not be the end state. The need to deploy better, more effective equipment to meet current and future threats will be an ongoing need for years to come. We must continue to invest in research and development for more effective equipment for screening passengers, their carry-on

and checked baggage, and air cargo. In the near term, TSA must develop and implement the next generation computer-assisted passenger prescreening system and transportation worker identification card program.

To the greatest extent practicable, TSA should test and evaluate promising security products operationally, using pilot programs at a variety of different size airports in several geographic and demographic areas, before committing large sums of money to full-rate-of-production contracts. This is important because pilot programs offer an opportunity to demonstrate clearly how the product will perform in its intended environment when used by typical operators.

At the same time, we should be responsible in how we spend our research and development funds. We found in our review of emerging security technologies and our audits of TSA contracts and procurements that TSA has much work to do to refine its deployment strategies and strengthen its procurement processes. In doing so, TSA will be able to better identify its equipment needs and maximize the Federal investment in security.

Carry Out Aggressive Covert Testing. An aggressive covert testing program should be implemented to evaluate the operational effectiveness of security systems and equipment. We understand that TSA has established such a program. Based on our findings concerning FAA's Red Team, TSA should ensure that it follows through and takes action when problems are identified. Effective implementation of the program will now be important and an area that warrants regular oversight by Congress and the DHS Inspector General.

Establish and Enforce Screener Performance Standards. The human factor has always been a "weak link" in aviation security. Since airport screeners are now TSA employees, TSA realizes it needs to develop, field test, and implement standards for measuring screener performance for various threat types using TIP and live testing. TSA implemented standards for selecting and training its screener workforce, and is formalizing an annual re-certification program for existing screeners. A prototype program is scheduled to begin in June 2003. This is particularly relevant since TSA is currently reducing the size of the screener workforce, and it makes the most sense that TSA should be releasing the weakest performers.

TSA must then execute a plan that includes comprehensive assessments and aggressive realistic testing to evaluate screener performance (checked baggage screeners and passenger and carry-on baggage screeners). This will help ensure the quality of the screener workforce. Further, because there are five airports under a pilot program using screening companies (which may later spread to more

airports), TSA will need to ensure that it has a program in place to certify private screening companies and their employees.

TSA should require air carriers, airport operators, and all other airport tenants to develop and implement comprehensive initial and recurring training programs to teach employees what their role in security is, the importance of their participation, how their performance will be evaluated, and what action will be taken if they fail to perform.

Improve Cargo Security. It is important for TSA to continue its efforts to improve cargo security. This includes strengthening the approval and re-approval process for indirect air carriers, and implementing a strategic plan to achieve the goal of screening cargo and mail. The Aviation and Transportation Security Act requires the screening of all cargo. One of the challenges facing TSA will be the development and deployment of certified machines to screen cargo. These costs may far exceed the costs to develop and deploy EDS.

That concludes my statement, Mr. Chairman. We have attached a listing of our testimonies, reports and investigations completed prior to September 11th. I would be pleased to address any questions you or other members of the Commission might have.

Attachment
(4 Pages)

AVIATION SECURITY TESTIMONY AND REPORTS
AS OF SEPTEMBER 14, 2001

TESTIMONY

Date	*Title*	*Report Number*
04/06/2000	Aviation Security Statement of Alexis Stefani, Assistant Inspector General for Auditing Before the Subcommittee on Aviation, Committee on Commerce, Science, and Transportation, U.S. Senate	AV-2000-076
03/16/2000	Aviation Security Statement of Alexis Stefani, Assistant Inspector General for Auditing Before the Subcommittee on Aviation, Committee on Transportation and Infrastructure, U.S. House of Representatives	AV-2000-070
03/01/2000	Improving Aviation Safety, Efficiency, and Security: FAA's Fiscal Year 2001 Request for Research, Engineering, and Development Statement of Alexis Stefani, Assistant Inspector General for Auditing Before the Subcommittee on Technology, Committee on Science, U.S. House of Representatives	AV-2000-054
03/10/1999	Aviation Security Statement of Alexis Stefani, Deputy Assistant Inspector General for Aviation Before the Subcommittee on Transportation and Related Agencies, Committee on Appropriations, U.S. House of Representatives	AV-1999-068
05/14/1998	Aviation Security Statement of Alexis Stefani, Deputy Assistant Inspector General for Aviation Before the Subcommittee on Aviation, Committee on Transportation and Infrastructure, U.S. House of Representatives	AV-1998-134

AVIATION SECURITY TESTIMONY AND REPORTS
AS OF SEPTEMBER 14, 2001

AUDIT REPORTS

Date	*Title*	*Report Number*
12/07/2000	Controls Over Airport Identification Media	AV-2001-010
11/18/1999	Airport Access Control	AV-2000-017
10/21/1999	Deployment of Explosives Detection Equipment	AV-2000-002
07/16/1999	Security of Checked Baggage on Flights Within the United States	AV-1999-113
10/05/1998	Deployment of Explosives Detection Systems	AV-1999-001
07/17/1998	Dangerous Goods/Cargo Security Program	AV-1998-178
06/01/1998	Management Advisory on Review of Security Controls Over Air Courier Shipments	AV-1998-149
04/17/1997	Federal Air Marshal Program	R9-FA-7-006
07/03/1996	Efforts to Improve Airport Security	R9-FA-6-014
09/20/1993	Audit of Airport Security	R9-FA-3-105

AVIATION SECURITY - INVESTIGATIONS
February 3, 1999 through September 14, 2001

Subject Area	*Date*	*Summary*
Screeners & Baggage Handlers	Sept. 14, 2001	Employees who are non-U.S. citizens without proper INS status were authorized to enter secured areas of Dulles, ongoing investigation.
Security Badges	Sept. 14, 2001	Arrest warrants were issued against non-U.S. citizens who obtained security badges at Miami International Airport.
Security Badges	Sept. 13, 2001	Employee at Miami International Airport pleads guilty to using job in ID section to make false security badges for coworkers.
Cockpit Access	June 7, 2001	Civilian used false FAA ID card to obtain unauthorized cockpit access on 3 separate flights.
Access Control	June 5, 2001	Non-employee of Miami International Airport illegally used an Airport Secured ID Display Area access badge to gain entry to a secured area.
Access Control	February 1, 2001	Miami International Airport employee gained access to secured areas by providing false data on Airport ID Badge application.
Screeners	October 25, 2000	Private firm (Argenbright) failed to conduct background checks on checkpoint screeners at Philadelphia Airport. Company fined $1 million, $350,000 restitution and $200,00 in investigative costs.
Access Control	May 1, 2000	Employees at Dallas-Ft. Worth Airport allowed unauthorized personnel to use their security badges to gain access to secured areas.

AVIATION SECURITY - INVESTIGATIONS
February 3, 1999 through September 14, 2001

Subject Area	*Date*	*Summary*
Screeners	March 27, 2000	Private firm (Aviation Safeguards) falsely certified on at least 70 occasions that criminal background checks had been accomplished on employees seeking access to secure areas at Miami International Airport.
Access Control	Feb. 3, 1999	Miami-Dade County Police Office falsely certified that criminal background checks had been accomplished on 22 employees seeking access to secure areas at Miami International Airport. Upon hiring, applicants had clearance to enter secured areas of the airport.