NAVAL POSTGRADUATE SCHOOL
Monterey, California

THESIS

AN ANALYSIS OF FEDERAL AIRPORT AND AIR CARRIER EMPLOYEE ACCESS CONTROL, SCREENING, AND TRAINING REGULATIONS

by

Edward G. Miller and Mark W. Dover

March, 1998

Principal Thesis Advisor:	David G. Brown
Associate Thesis Advisor:	Donald R. Eaton

Approved for public release; distribution is unlimited.

REPORT DOCUMENTATION PAGE

Form Approved
OMB No. 0704-0188

Public reporting burden for this collection of information is estimated to average 1 hour per response, including the time for reviewing instruction, searching existing data sources, gathering and maintaining the data needed, and completing and reviewing the collection of information. Send comments regarding this burden estimate or any other aspect of this collection of information, including suggestions for reducing this burden, to Washington headquarters Services, Directorate for Information Operations and Reports, 1215 Jefferson Davis Highway, Suite 1204, Arlington, VA 22202-4302, and to the Office of Management and Budget, Paperwork Reduction Project (0704-0188) Washington DC 20503.

1. AGENCY USE ONLY *(Leave blank)*	2. REPORT DATE March 1998	3. REPORT TYPE AND DATES COVERED Master's Thesis

4. TITLE AND SUBTITLE AN ANALYSIS OF FEDERAL AIRPORT AND AIR CARRIER EMPLOYEE ACCESS CONTROL, SCREENING, AND TRAINING REGULATIONS

5. FUNDING NUMBERS

6. AUTHOR(S) Edward G. Miller and Mark W. Dover

7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES)
Naval Postgraduate School
Monterey, CA 93943-5000

8. PERFORMING ORGANIZATION REPORT NUMBER

9. SPONSORING / MONITORING AGENCY NAME(S) AND ADDRESS(ES)

10. SPONSORING / MONITORING AGENCY REPORT NUMBER

11. SUPPLEMENTARY NOTES

The views expressed in this thesis are those of the authors and do not reflect the official policy or position of the Department of Defense or the U.S. Government.

12a. DISTRIBUTION / AVAILABILITY STATEMENT

Approved for public release; distribution is unlimited.

12b. DISTRIBUTION CODE

13. **ABSTRACT *(maximum 200 words)***

Current Federal Aviation Regulations concerning civil aviation security are focused on countering the threat of a passenger hijacking a commercial airplane. Current media and government emphasis is focused on a passenger breaching security at an airport in the U.S. and not an employee breaching security. The security of the U.S. air travel industry from terrorist attacks hinges on an effective civil aviation security program. Government and aviation industry officials would greatly benefit from the revision of the current Federal Aviation Regulations concerning civil aviation security to address the issue of terrorism initiated by an employee.

This thesis provides a thorough examination of current Federal Aviation Regulations parts 107 and 108 sections concerning airport and air carrier employee access control, screening, and training. Based upon field research of five U.S. airports, the work furthermore analyzes related issues and problems associated with these regulations and generates recommendations that serve to enhance security for the traveling public, air carriers, and persons employed by or conducting business at public airports.

14. SUBJECT TERMS
Airport Security, Federal Aviation Regulation Part 107, Federal Aviation Regulation Part 108

15. NUMBER OF PAGES
117

16. PRICE CODE

17. SECURITY CLASSIFICATION OF REPORT Unclassified	18. SECURITY CLASSIFICATION OF THIS PAGE Unclassified	19. SECURITY CLASSIFI- CATION OF ABSTRACT Unclassified	20. LIMITATION OF ABSTRACT UL

AN ANALYSIS OF FEDERAL AIRPORT AND AIR CARRIER EMPLOYEE ACCESS CONTROL, SCREENING, AND TRAINING REGULATIONS

Edward G. Miller - Lieutenant Commander, United States Navy
B.S., Embry Riddle Aeronautical University, 1986
and
Mark W. Dover, Lieutenant, United States Navy
B.S., Auburn University, 1991

Submitted in partial fulfillment of the
requirements for the degree of

MASTER OF SCIENCE IN MANAGEMENT

from the

NAVAL POSTGRADUATE SCHOOL
March 1998

Authors: ______________________ ______________________

Edward G. Miller Mark W. Dover

Approved by: ______________________

David G. Brown, Principal Thesis Advisor

____

Donald R. Eaton, Associate Thesis Advisor

____

Reuben T. Harris, Chairman
Department of Systems Management

ABSTRACT

Current Federal Aviation Regulations concerning civil aviation security are focused on countering the threat of a passenger hijacking a commercial airplane. Current media and government emphasis is focused on a passenger breaching security at an airport in the U.S. and not an employee breaching security. The security of the U.S. air travel industry from terrorist attacks hinges on an effective civil aviation security program. Government and aviation industry officials would greatly benefit from the revision of the current Federal Aviation Regulations concerning civil aviation security to address the issue of terrorism initiated by an employee.

This thesis provides a thorough examination of current Federal Aviation Regulations parts 107 and 108 sections concerning airport and air carrier employee access control, screening, and training. Based upon field research of five U.S. airports, the work furthermore analyzes related issues and problems associated with these regulations and generates recommendations that serve to enhance security for the traveling public, air carriers, and persons employed by or conducting business at public airports.

TABLE OF CONTENTS

LIST OF ACRONYMS

ACLU	American Civil Liberties Union
ACS	Aviation Civil Security
AFB	Air Force Base
AIP	Airport Improvement Program
AOA	Air Operations Area
ASC	Airport Security Coordinator
ASP	Airport Security Program
BIS	Biometric Identification System
CCTV	Closed Circuit Television
CJIS	Criminal Justice Information Services Division
DEA	Drug Enforcement Agency
DOS	Department Of State
DOT	Department Of Transportation
DOTIG	Department Of Transportation Inspector General
EA	Exclusive Area
EDS	Explosive Detection System
FAA	Federal Aviation Administration
FAR	Federal Aviation Regulation
FBI	Federal Bureau of Investigation

FY	Fiscal Year
GA	General Aviation
GAO	General Accounting Office
GPO	Government Printing Office
IG	Inspector General
IMS	Ion Mobility Spectroscope
INS	Immigration Naturalization Service
JFK	John F. Kennedy International Airport
LAA	Libyan Arab Airlines
LAX	Los Angeles International Airport
MSCR	Magnetic Stripe Card Reader
NAS	Naval Air Station
NCIC	National Crime Information Center
NCRC	National Crime Record Computer
OJT	On Job Training
PAN AM	Pan American Airlines
PC	Personal Computer
PCS	Proximity Card System
PSA	Pacific Southwest Airlines
R&D	Research and Development
SA	Secure Area

SFO	San Francisco International Airport
SIDA	Security Identification Display Area
TWA	Trans World Airlines
UAS	Universal Access System
US	United States

I. INTRODUCTION

The following is an analysis of current Federal Aviation Administration (FAA) regulations concerning airport and airport employee security and their application in the field. Our purpose is to analyze the effectiveness of the specific Federal Aviation Regulation (FAR) Parts 107 and 108 sections pertaining to Airport and Air Carrier Employee Access Control, Screening, and Training procedures.[1]

These regulations require each airport operator to implement and enforce airport security. Specifically, FAR 107 mandates implementation of an FAA approved Airport Security Program (ASP) by each individual airport that provides airport security for air carriers providing scheduled air service operations against the threat of hijacking. FAR 108 requires each airplane operator to implement and enforce procedures that protect aircraft and facilities providing scheduled air service operations against the threat of hijacking.

The intent of this thesis is to generate recommendations useful for enhancing security for the traveling public, air carriers, and persons employed by or conducting business at public airports by increasing employee awareness of and compliance with civil aviation security measures. This is important given that most media and government emphasis is currently focused on a *passenger* breaching security at an airport

[1] Research focuses on (1) Airport Access Control: sections 107.14 – Access Control System, 107.25 – Airport Identification Media, 108.13 – Security of Airplanes and Facilities, (2) Employee Screening: sections 107.2 and 108.4 – Falsification, 107.31 and 108.33 – Access investigation, and (3) Employee Training: section 108.31– Employment standards for screening personnel.

in the United States (U.S.) and not an *employee* breaching security. Incidents suggest security may be easily breached by a disgruntled or amoral employee. For purposes of this thesis, an *employee* is defined as any worker of an airport, airport tenant activity, or airline operating in or through the airport.

This first chapter provides a brief background history of FAR 107 and 108 and a summary of the terrorist threat and the need for secure air travel. It further discusses the significance of the research, research scope and method, and intended application of the thesis.

A. FAR 107 AND 108 BACKGROUND

In response to a rise of hijacking incidents, and to ensure the security of airports serving scheduled air carriers, the FAA issued FAR 107 on March 18, 1972 and FAR 108 on 15 January, 1981. These regulations require airports to implement prescribed security measures by developing and observing an airport specific security program. These regulations are primarily directed towards countering the threat of hijacking. However, since the inception of FAR 107 and 108 the terrorist threat has shifted from hijacking towards more lethal means of achieving terrorist goals.

In the last two decades, the hostile takeover of Trans World Airlines (TWA) flight 847 in Beirut, Lebanon, the devastating explosion of Pan American (Pan Am) flight 103 over Lockerbie, Scotland, and the recent destruction of TWA flight 800 have shown U.S. policy makers that our air transport industry is as vulnerable as the rest of the world to criminal acts of terrorism. The loss of TWA flight 800 served to renew the battle against air-terrorism. Even though the cause of this last disaster appears to be mechanical failure, the incident suggests that something must be done to prevent future air catastrophes.

B. THE TERRORIST THREAT AND THE NEED FOR SECURE AIR TRAVEL

Terrorists make it their business to threaten the most basic of human rights, the right to life. The civil aviation industry has, since its inception, been dedicated to protecting the overall safety of passengers and crews. It is the incredibly good safety record of the world's airlines that has helped to make air travel such a phenomenally successful mode of transport, and one of the fastest growing industries in the world. Even if there were no legal regulations on the airlines and airports to provide security, the industry would recognize the moral obligation resting on the government and the civil aviation community to take all reasonable measures to protect passengers, employees, and the public in general, against the threat of aviation terrorism.

The 1991 Arabian Gulf War demonstrated that if the public develops a real fear of flying and no longer trusts the capability of governments and aviation authorities to deter and prevent terrorist attacks, they will simply refuse to use the airlines as a travel mode. In the first week of the war the Association of European Airlines claimed that its members lost 25 percent of their traffic. Airline Business magazine estimated that the industry as whole was losing approximately 1.5 billion dollars per month in the immediate aftermath of the war. [Ref. 14: p.103] The industry has every reason to fear the effects of any future major conflict in the Middle East and the potential accompanying threat of increased terrorism. What counts is the public's perception of the risks involved. Whereas airlines used to argue that they could not afford effective security, they must now realize that they cannot afford not to have an effective aviation security system.

Government and the public have other powerful reasons, in addition to the principle of protecting the lives of the innocent, which should compel them to help create effective aviation security. The U.S. has a vital interest in the maintenance of lawful authority and the rule of law. By resorting to lethal tactics terrorists brutally defy the authority of the law. It would be absurd to argue that individual acts of aviation terrorism threaten the survival of the U.S. Yet it would also be irrational to deny that the U.S. has a vital interest in the defeat and eradication of groups that commit major crimes such as terrorism, and that weakness in responding to terrorist attacks may lead to the dangerous policy of making major concessions to terrorists, thus encouraging other terrorist groups to use similar tactics.

There is another major argument for establishing an effective aviation security system, and it is one which should add far greater urgency to our efforts. This suggests that the threat posed by aviation terrorists has become infinitely more lethal over the past decade. Twenty years ago the major terrorist threat to aviation was hijacking, a problem that has by no means disappeared. However, the danger of hijacking has been sharply reduced by a combination of simple but effective technology, procedures, and the deterrent effect of inescapable apprehension or death of the hijackers upon landing of the affected aircraft.

Over the past two decades terrorists have switched the emphasis away from hijacking to other more lethal means. This includes smuggling a bomb on board an airliner and timing it to explode in mid air, as was demonstrated in the horror of the Pan Am flight 103 disaster. When a bomb explodes on an airliner at an altitude of over 30,000 feet, the passengers and crew have no chance of survival. The potential for very much higher levels of casualties exist if an airliner were to be blown up above a major population center. Modern plastic explosives and sophisticated timing mechanisms provide an ideal terrorist weapon for this purpose. The huge payload capacities of modern jumbo jets serve to maximize the carnage.

Federal Aviation Regulations (FAR) 107 and 108 are geared primarily to confront the hijacking threat. The magnetometer archways and X ray machines introduced in the early 1970's were designed to prevent passengers from smuggling metallic objects and potential hijack weapons on board aircraft. Although the sabotage bomb threat has become more of a reality over the last decade, the U.S. has moved lethargically in implementing an Explosive Detection System (EDS), stringent baggage screening procedures, effective perimeter and access controls, and other necessary countermeasures.

As an example, an airline that is fully capable of coping with this new challenge is El Al Airlines of Israel. El Al compensates for a lack of technologically advanced equipment by exploiting their unique assets in counter-terrorism intelligence, passenger profiling and interrogation, and a comprehensive manual luggage screen. Although much can be learned from El Al in terms of intelligence, motivation and the importance of the human factor in aviation security, it would be totally impracticable for the U.S. to adopt El Al's overall approach. El Al has much less air traffic, no short haul flights, and its passengers are sufficiently motivated to accept much earlier check-in times than would be customary for U.S. airlines. Nevertheless, the U.S. must adopt a plan of attack to counter the current and future threat of air terrorism.

C. SIGNIFICANCE OF THE RESEARCH

Terrorism has been, for the most part, a phenomenon afflicting U.S. interests overseas, and the threat to U.S. civil aviation is assessed to be higher abroad than it is domestically. However, the World Trade Center bombing in February 1993 indicates that terrorism is also a very real threat in the United States, and may be on the rise.

The number of international terrorist attacks against U.S. interests rose between 1995 and 1996 more than 66 percent. [Ref. 8:p.8] The Department Of State (DOS) asserts that U.S. domestic targets are not immune to international terrorism, describing the terrorist threat as "real and potentially lethal." The DOS views these developments as cause for concern.

Given the increased demand for air travel in the last decade and the more lethal tactics of terrorists, a thorough analysis of FAR 107 and 108 concerning airport and air carrier employee access control, screening, and training is necessary to assure that the U.S. is prepared to counter the threat of terrorism in the future.

D. RESEARCH SCOPE AND METHOD

This research is confined primarily to the analysis of FAR 107 and 108 Airport and Air Carrier Employee Access Control, Employee Screening, and Employee Training. Research data concerning FAR 107 and 108 were gathered from the following sources:

1. Published studies and literature from the Federal Register, Government Printing Office (GPO), FAA Office of Civil Aviation Security (ACS), General Accounting Office (GAO), DOT office of IG, DOS, libraries and current press reports.
2. Statements gained from interviews with U.S. airport management and security officials.
3. Statements gained from interviews with U.S. Federal Bureau of Investigation (FBI) and FAA agents.

Thesis conclusions are partly based upon opinions advanced by these sources.

E. RESEARCH APPLICATION

The FAA and U.S. airports, in particular, are the intended primary beneficiaries of this research. The FAA, and airport officials and planners may be able to apply the information gained to possibly improve the overall security of the U.S. air travel system. Through these recommendations, a more effective practice of individual and corporate responsibility for complying with security regulations may be achieved for all U.S. Category X, One, Two, Three, Four and Five airports. The Department Of Defense (DOD) may also benefit from these findings in managing the operations of common user air lift terminals such as Naval Air Station (NAS) Norfolk, Dover Air Force Base (AFB), and Travis AFB.

II. FAR 107 AND 108 DEVELOPMENT

A proper understanding of a Federal Aviation Regulation (FAR) requires knowledge of the important issues surrounding its development. This chapter, therefore, provides a background summary of FAR 107 and 108, a presentation of significant employee–initiated security incidents relating to employee security and a plain language description of these regulations.

A. FAR 107 AND 108 BACKGROUND

Created in 1958 under the Federal Aviation Act (Public Law 85-726), the Federal Aviation Administration (FAA) is responsible for ensuring the safety and security of air travel. Specifically, the Federal Aviation Act directs the Administrator of the FAA to prescribe regulations requiring the screening of all passengers and carry on baggage for weapons, and requires regulations to protect persons and property aboard aircraft from acts of criminal violence and piracy.

As part of that mission, the FAA Office of Civil Aviation Security (ACS) was established to issue security requirements, inspect airline and airport security operations and issue civil penalties for noncompliance with those requirements. At U.S. airports, security is designed as a joint endeavor between airport and airplane operators.

The first hijacking of a U.S. flag air carrier occurred in 1961. The U.S. Congress responded to this threat by issuing the Arms Export Control Act as a means to counter the proliferation of armed passengers on all flights in or out of the U.S. [Ref. 2:p.27] As a means to provide further direction to the operators and to secure the industry against the growing threat of hijacking, the FAA issued FAR 107 on 18 March 1972.

The U.S. aviation security system that has evolved since the passage of FAR 107 has been fundamentally effective in countering the threat of terrorism. This is significant considering the tremendous growth of the air travel industry and the number of air carriers over the last two decades both domestically and internationally, mainly due to the passage of the Airline Deregulation Act of 1977. This growth in the number of air carriers following economic deregulation of the air industry prompted the FAA to release FAR 108 on 15 January, 1981 in order to provide air carriers with their own set of regulations, specifically designed to provide quidance in countering the threat of hijacking.

FAR 107 and 108 have been amended on several occasions, but they have never undergone a comprehensive update. Tragic events such as Pan American Airlines (Pan Am) flight 103 and Trans World Airlines (TWA) flight 800 led to unified efforts from government and industry officials to strengthen aviation security around the world, particularly at U.S. airports. The FAA responded to these events by issuing emergency amendments to airport security programs, citing FAR 107 and 108 authority.

The destruction of Pan Am flight 103 on 21 December, 1988 prompted a series of recommendations from the Bush Commission to improve and change specific civil aviation security regulations. Most of these recommendations became law with the Aviation Security Improvement Act (Public Law 101–604), enacted 16 November 1990.

This Act specifically required the FAA to accomplish the following milestones no later than November 1993: [Ref. 2:p.24]

1. Speed up explosives-detection equipment research and development.
2. Heighten background security checks on airport personnel.
3. Facilitate the public release of passenger manifests within three hours of a crash.

The Bush Commission was critical of the domestic U.S. civil aviation security system for failing to provide the proper level of protection for the traveling public and urged major reforms. Additionally, the Bush Commission recommended that the FAA immediately initiate the planning and analysis necessary to phase additional security measures into the domestic air travel system. [Ref. 2:p.27] The 1990 Act mandated many changes to airport and air carrier security programs, as well as federal staffing and reporting procedures. Several directives were initiated to impose screening standards for air crew and security personnel, and training standards and criminal history checks for certain airport and air carrier personnel. The law also required the FAA to coordinate with the Federal Bureau of Investigation (FBI) to assess the domestic air transport system, develop security guidelines for airport design and construction, and expand the security technology research and development program.

In September 1993, the Department Of Transportation (DOT) office of Inspector General (IG) issued a report critical of certain aspects of the FAA's oversight of airport security systems. [Ref. 3] This report found significant deficiencies in the effectiveness of employee access control and challenge procedures at five U.S. airports. It also recommended that airport and air carrier implementation of procedures for access control and challenge be strengthened, stressing that the FAA must take steps to increase airport and air carrier employees' awareness and responsibility for those procedures. The overall conclusion of this report ultimately criticized the FAA's security regulations, calling them "inadequate." [Ref. 3:p.ii] The assessment criteria for this report were obtained from a series of DOTIG undercover investigations at some of the nation's busiest international airports. For example, in fifteen of twenty attempts to gain access to posted airport secure areas, DOTIG agents entered aircraft parking areas and baggage areas, and on one occasion an unarmed hand grenade was passed undetected through a metal detector.

In January 1994, the FAA responded to the 1993 DOTIG report by meeting with representatives of airports, air carriers, airport tenants, employee groups and aviation worker unions to discuss the report's findings and to emphasize the need for improved employee security awareness. Simultaneously, the FAA began focused inspections at U.S. airports with the highest volume and most complex security operations. Slated to continue on a routine basis, these special inspections target access control, the security measure that the DOTIG found to be a universal weakness.

Also in January 1994, the General Accounting Office (GAO) issued a report suggesting further actions the FAA could take to improve civil aviation security. [Ref. 7] This report was issued in response to a Congressional inquiry on the FAA's efforts to implement the Aviation Security Improvement Act. This report found that the milestones mandated by the Act were not achieved on time by the FAA on time. As a rebuttal to this failure, the FAA accused Congress of setting overly-stringent standards and requiring complicated tests of the new technologies, even though the milestone completion deadlines were almost five years after the Pan Am disaster. The GAO did find, however, that the FAA had taken some of the most important steps in response to the Act, but noted that additional steps must be taken to enhance FAA security programs and initiatives. These actions include:

1. Pilot-testing new procedures before implementation.
2. Strengthening human factors research and its application.
3. Making systematic analytical use of information that the FAA collects during air carrier and airport security inspections.
4. Providing airport security coordinators with security clearances, so that they can be given classified information regarding threats to civil aviation.

Similar to the 1993 DOTIG report, the GAO report highlighted the need for the FAA to increase industry employees' overall awareness of security measures. The report concluded that the FAA must refine security training and procedures to increase employee sensitivity to security requirements.

The FAA maintains that all provisions of the 1990 Act have been fully implemented. However, the DOTIG office completed a follow up report in July 1996 that presented evidence which contradicts the FAA's position. [Ref. 4:p.8] This report found that many of the same problems identified in the 1993 DOTIG report were still present, and the 1990 Act did not achieve the required milestones to counter air-terrorism.

As security tightened throughout the nation's airports in the wake of the 1996 TWA flight 800 disaster, the Clinton Administration enacted Executive Order 13015 and established the White House Commission on Aviation Safety and Security headed by Vice President Gore (Gore Commission). [Ref. 1:p.3] The Gore Commission produced a response plan to this incident that contained twenty recommendations and eighteen projects that are geared to serve as the new antidote for this threat. This response plan was enacted by the President to supplement the 1990 Aviation Security Improvement Act.

Given the realities exposed by these reports, and the aviation disasters to date, countering air-terrorism has become a fundamental concern of the aviation industry. The Gore Commission states in its Final Report to the President that the threat against civil aviation is changing and growing, and that the federal government must lead the fight against it. It recommends that the federal government commit greater resources to improving aviation security and work more cooperatively with the private sector and local law enforcement authorities in carrying out security responsibilities.

In passing the Fiscal Year (FY) 1997 Federal spending bill in September 1996, Congress approved $429.4 million for aviation counter terrorism support that is part of a $1.1 billion total counter terrorism package. It is the first piece of what could become a $6 billion counter terrorism expenditure over the next ten years. [Ref. 5:p.33]

For the six hundred million passengers that utilize the U.S. civil aviation system annually, the implications of such an expenditure may be enormous. The industry may seriously confront the challenge of retaining convenience, competitive pricing and ease of passenger movement in the midst of increased security. As a whole, the passenger air industry is currently seeking to address the weaknesses identified in the Gore report and improve compliance. In particular, many airports and air carriers have begun improving their training programs and instituted programs to provide individual incentives for compliance including escalating disciplinary action for instances of non-compliance. The FAA proposes to implement similar measures at other airports by clarifying and modifying airport access control, employee screening, and employee training requirements.

B. SIGNIFICANT INCIDENTS

Since the inception of FAR 107 and 108, the primary threat to civil aviation has evolved beyond hijacking to bombing of aircraft and murderous attacks within airports. The following presentation of significant employee, or impersonated employee–initiated security incidents are indicative of this evolution: [Ref. 12:p.16]

1. September 5, 1986: Terrorist assault on Pan Am Flight 73. Four terrorists assaulted Flight 73 in Karachi, Pakistan as the aircraft waited to take off. The four terrorists were dressed as airport security personnel and drove an airport security vehicle alongside the aircraft. The terrorists stormed the aircraft and after 17 hours of negotiations, the aircraft's auxiliary power unit failed. Anticipating an attack by security

forces, the terrorists opened fire on the massed passengers, killing 22 persons and injuring 125 others before security forces could intervene.

2. December 7, 1987: Destruction of Pacific Southwest Airlines (PSA) Flight 1771. Flight 1771 crashed when a recently terminated airline employee boarded the Los Angeles to San Francisco flight with a handgun, shot one passenger (his former supervisor), the flight crew, one flight attendant, and presumably himself while the flight was airborne. As a result, all 38 passengers and five crew on board were killed. The terminated employee had managed to retain his airline identification after his dismissal and used it to bypass the passenger screening checkpoint.

3. December 21, 1988: The bombing of Pan Am Flight 103. All 243 passengers and 16 crew on board, plus 11 persons on the ground at Lockerbie, Scotland, were killed. Subsequent inspection of the reconstructed aircraft determined that a device consisting of plastic explosives hidden inside a tape cassette player was responsible for its destruction. The device had been concealed in checked luggage. Individuals working for the Government of Libya are thought to be responsible for the bombing. One probable conspirator was the former manager of the Libyan Arab Airlines (LAA) office in Valletta, Malta and had retained full access to the airport after his dismissal. Using this access privilege and other knowledge gained as representatives of LAA, the conspirators bypassed security checks at Valletta's Luqa Airport and inserted the suitcase containing the bomb into baggage of an Air Malta flight to Frankfurt. The bomb was a time delay type and was scheduled to detonate over the Atlantic Ocean, however, the terrorist's

calculations were wrong.

4. August 14, 1990: Gunman gained unauthorized access to the Air Operations Area (AOA) at Washington National Airport. The gunman, armed with a .38 caliber revolver, entered the Ogden Allied Services garage and held several employees at gunpoint. The gunman was a former employee at Ogden and had voluntarily left his job. He commandeered a fuel truck, forced an Ogden employee to drive onto the AOA and commenced firing several shots at a second Ogden fuel truck, wounding two persons. He was in possession of 30 to 40 rounds of ammunition when he was arrested. A molotov cocktail was also recovered from the commandeered fuel truck, and several other ones were found in the gunman's vehicle.

These are but four of the two hundred and eighty nine terrorist attacks that have been reported by airports throughout the world during the past 5 years. These attacks have included 59 airport attacks, 4 bombings and shootings onboard aircraft, 28 shootings at aircraft, 79 commandeering's, 89 hijacking's, 28 general aviation (GA) incidents and 79 off airport attacks. At least 41 persons have been killed and more than 250 injured in attacks at airports between 1992 and 1996. [Ref. 6:p.83]

C. FAR 107 AND 108 SUMMARIES

Sections of FAR 107 and 108 specifically pertaining to Airport and Air Carrier Employee Access Control, Employee Screening, and Employee Training procedures are provided in the following paragraphs in plain language format. In general, FAR 107 mandates implementation of an FAA approved Airport Security Program (ASP) that provides security of airports, for air carriers providing scheduled air service operations, and against the threat of hijacking. FAR 108 requires each air carrier to implement and enforce procedures that protect aircraft and facilities providing scheduled air service operations against the threat of hijacking. The current regulations, in their official FAA language, are provided in the Appendix for reader reference.

1. Employee Access Control

Sections 107.14–Access Control System, 107.25–Airport Identification Media, and 108.13–Security of Airplanes and Facilities all pertain to the issue of exercising authority over employee access to all secured areas included within the AOA of a U.S. airport.

Section 107.14 mandates a security plan for perimeter boundaries of the airport to be implemented by the airport operator. This security must be a system, method, or procedure which meets FAA requirements for controlling access to secured areas of airports. To differentiate between persons authorized to have access to particular portions of the secured areas and persons authorized to have access only to other portions or to the entire secured area, the system, method, or procedure shall be capable of limiting an individual's access by time and date.

Section 107.25 establishes minimum security standards for the issuance of airport identification media to airport employees operating within the Security Identification Display Area (SIDA). It prescribes directives that prevent the issuance of media that allows unescorted access to this area unless the proper FAA approved SIDA training has been completed and documented by the Airport Security Coordinator (ASC).

Section 108.13 provides guidance for the airport to mandate the implementation of the ASP by all air carriers in their airplanes and facilities. It gives guidance to air carriers to prohibit unauthorized access to the airplane, for a responsible agent to properly inspect and handle all baggage, to require identification of persons shipping goods or cargo onboard an airplane, to handle all goods and cargo so as to prohibit unauthorized access, and to conduct a preflight security inspection of the airplane.

2. Employee Screening

Sections 107.2 and 108.4–Falsification, and 107.31 and 108.33–Access Investigation all pertain to the issue of employee screening procedures at a U.S. airport. The sections regarding Falsification and Access Investigation have been combined in this presentation because they are verbatim in their official form.

Sections 107.2 and 108.4 address the possibility of fraudulent or intentionally false statements made by airport and air carrier employment applicants in their employee screening records. This section is intended to provide a firm means for the FAA to take legal enforcement action against individuals who make such statements in employment applications.

Sections 107.31 and 108.33 require airport and airplane operators to conduct a pre–employment investigation of applicants to disqualify individuals convicted of certain enumerated crimes from having, or being able to authorize others to have, unescorted access privileges to a SIDA of a U.S. airport. These standards delineate specific items required of employers in order to prevent the hiring of individuals that have committed crimes as listed in these sections. This section also mandates that individuals undergo a review that explains their previous 10 years of employment history. This is in conjunction with verification of the previous 5 years of history conducted by the potential employer which includes verification of employment data by the individual's previous employer in writing, by documentation, telephone, or in person. This section also prescribes that if a 12 month gap in employment exists within the individual's 10 year employment history verification or if the individual can not support statements made in the 5 year verification, then the individual is required to explain these discrepancies and the potential employer may request a check of the individual's fingerprints held by the FBI.

3. Employee Training

Section 108.13 mandates minimum employment standards required of employees in capacities that are involved with the screening of passengers and baggage in U.S. airports. These standards include education and experience, aptitudes, physical coordination, visual and aural acuity, color perception, and motor skills. These requirements are necessary in order to properly operate screening equipment, hear and respond to alarms and instructions, conduct physical searches, and write reports.

III. THE U.S. AIRPORT SYSTEM

A detailed analysis of Federal Aviation Regulations (FAR) 107 and 108, and their implementation, requires some understanding of the specific security characteristics of U.S. airports. This chapter therefore provides a profile of the current U.S. airport security system by discussing the following:

A. Operational classification of airports.

B. Security classification of airports.

C. Security responsibilities.

D. Classification of security areas.

E. Security alert levels.

F. Security tools.

A. OPERATIONAL CLASSIFICATION OF AIRPORTS

Airports are classified into three categories according to the annual level of passenger boardings (enplanements) the airport conducts. This classification system assists the Department Of Transportation (DOT) in identifying airports that serve public air transportation, that are critical to supporting national security, and that are eligible for federal aid. [Ref. 15:p.36] The three airport operational categories are: 1) commercial service, 2) general aviation (GA), and 3) reliever.

Commercial service airports receive scheduled passenger service and have 2,500 or more annual passenger boardings. There are currently 566 commercial service airports in the U.S. Commercial airports are partitioned into two sub-classifications: 1) Primary, and 2) Other. Primary Airports are commercial service airports with 10,000 or more annual enplanements. There are currently 417 primary commercial service airports in the U.S. The remaining 149 commercial airports are classified as Other commercial service airports with 2,500 to 10,000 annual enplanements.

General aviation (GA) airports are those with fewer than 2,500 annual enplanements. There are currently 2,424 GA airports in the U.S. Reliever Airports are a special category of GA airports that are located in the vicinity of major commercial airports. These airports are specifically designated by the FAA as GA airports that provide relief to congested major airports. To be classified as a reliever airport, the airport must have at least 50 permanent based aircraft, manage 25,000 itinerant operations from other airports or 35,000 unscheduled transient aircraft operations within the last two years. [Ref. 15:p.36] There are currently 329 reliever airports in the U.S.

B. SECURITY CLASSIFICATION OF AIRPORTS

Unlike the operational classification, airports are also classified into six security categories according to the annual number of passengers screened for security purposes. The six airport security categories are Category X, and Category One through Five.

Airports that require the highest level of security are Category X. Currently 19 U.S. airports retain this classification. The following types of airports may be designated Category X:

1. Airports where 25 million or more persons are screened annually.

2. Airports having 1 million or more international enplanements.
3. Airports with special considerations (e.g.; history of incidents, airports in unique locations such as those serving Washington, D.C.).

Category One airports are those where more than 2 million persons are screened annually. Category Two airports are those with at least 500,000 but less than 2 million persons screened annually. Category Three airports are those with less than 500,000 persons screened annually. Category Four airports are those that conduct screening for flights that deplane passengers into a Sterile Area (SA) at another airport, in this case the total number of persons screened is insignificant. Category Five airports are those where screening is not required and that serve aircraft seating 31 through 60 passengers.

C. SECURITY RESPONSIBILITIES

Provision of security in U.S. air travel is the responsibility of: 1) the FAA, 2) airports, and 3) air carriers.

1. Federal Aviation Administration (FAA)

The FAA is responsible for ensuring the safety of air travel through the establishment of security requirements, inspection of airline and airport security operations, and by issuing civil penalties for noncompliance with those requirements. The operational role of the FAA in airport security is limited to the dissemination of intelligence and threat information.

2. Airports

Airports are responsible for security on airport property. They are charged with providing a secure operational environment for the air carrier. To achieve this, the FAA has established security requirements for the response of law enforcement to various security threats, physical security such as airport perimeter fencing, and access restrictions to operations areas. Specifically, airports are responsible for securing access to the Airport Operations Area (AOA) by controlling the movement of persons and vehicles and providing the general law enforcement response to any security breaches or problems.

3. Air Carriers

Air carriers are responsible for the most visible security measures. These measures include the screening of passengers and carry-on baggage, including training and testing of persons responsible for the screening, securing the aircraft against the introduction of any explosive or incendiary devices, monitoring and securing all sterile areas under their control, and controlling the handling and loading of baggage and cargo. [Ref. 2:p.47] Air carriers may contract with private security firms to perform this function, and the carriers at a given airport will often work together. Nevertheless, the FAA holds the individual air carriers accountable for the effectiveness of screening operations.

D. CLASSIFICATION OF SECURITY AREAS

Effective security areas are a critical cornerstone of airport security. This requires clear definition of security areas, establishment of baseline security requirements for designated areas, and effective enforcement of established security procedures for these areas. The FAA has identified five such security areas: 1) Air Operations Area (AOA), 2) Secure Area (SA), 3) Security Identification Display Area (SIDA), 4) Sterile Area, and 5) Exclusive Area (EA).

1. Air Operations Area

As explained in FAR 107, airport operators are required to designate a portion of the airport where security measures are applied to protect areas used for landing, taking off, or surface maneuvering of airplanes. As defined, the AOA encompasses the (1) runway, (2) taxiway, (3) ramp, (4) parking, (5) tarmac, and (6) undeveloped areas within the airport perimeter.

FAR 107.13 defines requirements for operators of airports serving scheduled passenger operations where the certificate holder of air carrier is required to conduct passenger screening under a program required by FAR 108. Airports shall use the procedures included, and the facilities and equipment described in its approved Airport Security Plan (ASP), to perform the following functions:

1. Control access to the AOA, including methods for preventing the entry of unauthorized persons and ground vehicles.

2. Control movement of persons and ground vehicles within each AOA, including, when appropriate, requirements for the display of identification.
3. Prompt detection and action to control each penetration, or attempted penetration, of an AOA by person whose entry is not authorized in accordance with the Airport Security Program (ASP).

2. Secure Area

The Secure Area (SA) was created by the issuance of FAR 107.14 in January 1989 in response to the 1987 Pacific Southwest Airlines (PSA) disaster (discussed in Chapter II). The SA encompasses the area where air carriers enplane passengers, deplane passengers, sort and load baggage, and any adjacent areas that are not separated by security controls or physical barriers. [Ref. 16:p.4] Under FAR 107.14, access control systems must:

1. Ensure that only authorized persons gain access to the SA.
2. Immediately deny access to persons whose authorization is revoked.
3. Differentiate between persons with unlimited access to the SA and persons with only partial access.
4. Be capable of limiting access by time and date.

3. Security Identification Display Area

Almost three years after FAA required airports to designate the Secure Area within airports, they mandated airport operators to implement additional identification display and training procedures to provide even more protection to carrier aircraft within a portion of the AOA. This new area, designated the Security Identification Display Area (SIDA), includes portions of the AOA which overlap with the SA. Per FAR 107.25, this area is defined as any area identified in the airport security program as requiring each person to continuously display on their outermost garment, an airport-approved identification medium unless under airport-approved escort.

SIDA areas vary from airport to airport. For example, San Francisco/Oakland (SFO) International Airport designates the entire AOA a SIDA, whereas Los Angeles (LAX) International Airport designates only specific areas of the AOA as SIDA.

Though designated SIDA areas vary per airport, FAA requirements do not. Per FAR 107.23 no airport may issue to any person any identification media that provides unescorted access to any SIDA unless the person has successfully completed training in accordance with an FAA-approved curriculum specified in the ASP. The curriculum specified in the ASP shall detail the methods of instruction, provide attendees the opportunity to ask questions, and include at least the following topics:

1. Control, use, and display of airport-approved identification or media.
2. Challenge procedures and the law enforcement response which supports the challenge procedures.
3. Restrictions on divulging information concerning an act of unlawful interference with civil aviation if such information is likely to jeopardize the safety of domestic or international aviation.

4. Non-disclosure of information regarding the airports security system or any airport tenant's security systems.
5. Other topics deemed necessary by the Assistant Administrator for Civil Aviation Security (ACS).

No person may use any airport approved identification medium that provides unescorted access to any SIDA unless that medium was issued to that person by the appropriate airport authority or other entity whose identification is approved by the airport operator. Examples of "other entities" include the FAA, U.S. Customs, and tenant air carriers. The airport operator shall maintain a record of all training given to each person under this section until 180 days after the termination of that person's unescorted access privileges.

4. Sterile Area

Per FAR 108.3, the Sterile Area is an area to which access is controlled by the inspection of persons and property in accordance with an approved security program used in accordance with FAR 129.25. Specifically the Sterile Area is the public area entered after passing through passenger screening checkpoints. Security of the Sterile Area is the responsibility of the air carriers.

5. Exclusive Area

The Exclusive Area (EA) is a dedicated area for which carriers are responsible for physical security in their operational areas leased from the airport. This area includes air operations, cargo buildings and airline spaces within the terminal building. Specific responsibilities include the SIDA requirements, access control system hardware, and procedures identified in the FAA approved ASP.

E. SECURITY ALERT LEVELS

In order to ensure that the FAA, airport operators, and air carriers are able to respond on short notice to civil aviation threats, a system of four security alert levels was devised. Security alert levels are comprised of a myriad of contingency action plans devised for identified threats and vary according to the severity of the threat. Contingency responses can be as subtle as increasing the number of on duty security personnel or as stringent as disallowing curbside check-in, prohibiting visitors from security areas and/or physical hand searches of all baggage. The FAA is responsible for declaring alert levels and contingencies to put in place. The FAA uses two tools for threat notification and contingency requirements: 1) Security Directives for air carriers, and 2) Emergency ASP amendments for airports, both of which are time based. Expiration dates trigger a timely review of the threat and determine continuance, modification, or elimination of a countermeasure.

The FAA has the authority to direct the implementation of actions at specific operations (airports/air carriers) subject to the threat, instead of industry wide. The security levels are listed below according to the severity of the threat, with Level One being the least severe and Level Four being the most severe:

1. Level One is implemented when current political tensions may lead to hostile demonstrations or low level attacks against U. S. citizens or interests.

2. Level Two indicates that there is information that suggests that groups known to have attacked civil aviation may be preparing actions against U.S. citizens or interests or civil disturbances which could affect civil aviation.
3. Level Three indicates that there is information that a terrorist group or hostile entity with known capability of attacking civil aviation is likely to carry out attacks against U.S. interests, or that civil disturbances with a direct impact on civil aviation have begun or are imminent.
4. Level Four is the highest threat level. This level is implemented when available information confirms that terrorist organizations with demonstrated capability are planning an attack against U.S. civil aviation and the highest level of security possible is required to protect U.S. air travelers.

F. AIRPORT SECURITY TOOLS

As indicated in the news media and current literature, there is no technological "silver bullet" available today to solve the complexities of airport security. The only true silver bullet is a system of layered defenses which terrorists must successfully infiltrate to reach their objective(s). The structure of a layered defense is unique to each airport facility, but the common requirement of all airport facilities is interaction of human resources and technology. Technology being used across the U.S. today is a combination of both old and new systems. This section provides descriptions of the following technologies currently employed in some, but not all, U.S. airports: 1) Electronic

Detection System, 2) Conventional Weapon Detection, 3) X-ray, and 4) Security Access Control.

1. Electronic Detection System

Plastic explosives have replaced guns, knives, and dynamite as terrorist weapons of choice. SEMTEX and C4, two of the most common brands of plastic explosives, pose serious problems for traditional metal detection systems because they have no metal content. Early Explosive Detection Systems (EDS) specifically designed to detect SEMTEX and C4 had high false positive rates making them unsuitable for employment. Today a technological breakthrough in EDS has yet to be discovered, however, the two systems currently being tested in Category X airports, have shown promise.

a. InVision CTX-5000

The InVision CTX-5000 is the only luggage screening device certified by the FAA as an EDS for plastic explosives and other weapons that are essentially "invisible" to all previously utilized security equipment. The CTX 5000 offers a three-dimensional slice through the suitcase, like a medical CAT scan, that gives information on both the shape and density of materials, and can automatically alert an security employee to suspicious objects. [Ref. 17:p.4]

This new technology has proven to be a significant technological advance in bomb detection, and is being fielded throughout the world. Though large (6 ft. x 14 ft.), costly ($1,000,000 per unit), and relatively slow (150 bags per hour), thirty-two CTX units have been sold worldwide. Only five CTX units are in operation at category X airports in the United States today, three of which are located at SFO, Atlanta-Hartsfield, and New York's John F. Kennedy (JFK). This is due to FAA funding constraints, and the U.S. government's classification of this technology as a research and development project instead of a procurement project.

b. Ion Mobility Spectroscope (IMS)

While the CTX 5000 searches for large concentrations of explosives, portable trace detection systems are used to detect small or trace amounts of explosive material. Commonly known as "sniffers" these detectors are used for screening passengers and carry-on baggage for minute amounts of chemicals. Portable systems of this type are actively being used at sterile area screening points in some Category X airports. IMS screening is performed on suspect as well as randomly selected baggage.

2. Weapon Detection

Since 1972 the U.S. has been utilizing Magnetometers (metal detectors) to search passengers for detection of firearms, knives and other metal-based weapons. Magnometers have proven to be a highly successful in thwarting hijacking. However, these devices were not designed for nor can they detect explosives. All passengers must be screened prior to entering the sterile area through use of a stationary walk-through device. Hand held magnetometer devices are used to pinpoint magnetic based items on individuals who fail walk through screening.

3. X ray

As with Magnetometers, x-ray devices have been in use since the early 1970's as the primary weapon detection device. Displayed images indicate object density, and image interpretation is a function of the screeners' training and abilities. All carry-on items and checked international baggage are required to undergo x-ray screening, however, checked domestic baggage is not. [Ref. 13]

4. Security area access control

Key to an effective access control program is positive control of security areas. Airports have installed different types of equipment in different locations. Some airports screen persons at checkpoints, while other airports have installed controls on doors beyond such checkpoints. Some airports have installed controls on both sides of doors leading into and out of the security area. [Ref. 16:p.5]

To secure doors and gates, magnetic stripe card readers (with and without integrated key pads), proximity card readers, biometric readers, electronic fences and passenger exit lanes control systems are utilized. Some airports have guarded gates with magnetic stripe card readers to separate passenger and cargo operations areas. Additionally, some airports have mounted closed circuit television cameras at doors and gates while others have chosen not to install such technology. [Ref. 16:p.5]

This subsection describes the types of technology available for use in an access control system:

a. Magnetic Stripe Card Readers (MSCR)

MSCR have been in existence since the early 1960's for control of entry points. The heart of a MSCR system is a central mainframe computer or an integrated network of Personal Computers (PC). Individually issued magnetic stripe cards (magnetic media) act as keys to access the system. [Ref. 18:p.1] With this system the employee "swipes" the magnetic media through the reader to open the controlled door or gate.

Advantages of a MSCR system is speed and ease of changing entry access codes, control of access through date and time, digital database of personnel accessing specific areas, and difficulty of duplicating cards. [Ref. 18:p.2]

b. MSCR with integrated keypad

Essentially the same system as a MCSR except personalized codes must be entered in unison with swiping of a magnetic media. This system reduces the possibility of area access by individuals using stolen or misplaced media.

c. Proximity Card System (PCS)

PCS uses infrared technology for area access. PCS manufactures use data transmission and encryption methods between the tag and reader that can't be counterfeited. With this system, the employee holds the card within a few feet of the reader to gain access. Unlike a MCSR, media proximity media never touches the reader and therefore wear is not a function of usage. Ease of use, convenience, speed and maintainability are notable qualities of this system. Many MCSR systems are being replaced by PCS systems. [Ref. 18:p.2]

d. Biometric Identification System (BIS)

BIS is a state-of-the-art security system. Two of the most common BIS techniques are retinal scan and hand scan. While retinal scan systems identify individuals by unique retinal properties, a hand scanner maps hand geometry using Three Dimensional (3D) techniques. [Ref. 28:p.1] While both systems are available, only the hand scan system is currently being used in U.S. airports today. San Francisco International (SFO) is one such airport using this technology.

e. Electronic fence

Airports with general aviation (GA) facilities have unique access control problems. General aviation, unlike airport and air carriers, is made up of local and transient civilian private pilots, self-employed mechanics, and Fixed Base Operator employees. In order for GA to operate in a SIDA, all users would require SIDA media. This would be a challenging if not impossible endeavor to manage. To facilitate the airport's airport security plans and eliminate SIDA requirements, electronic fences are being used at some airports. Electronic fences are invisible barriers that use sensors to detect movement and trigger an alarm to alert security personnel when breached.

f. Passenger Exit Lane Control System

This system is designed to prevent entry into Sterile Areas through exit lanes. The motion-sensor system issues an audible warning, flashes security lighting and produces a photo of the individual within seconds of activation. The system is independent of breach speed (walk, run, crawl) and can catch a person going the wrong way against a crowd of as many as 20 persons. This system is currently installed at SFO and Minneapolis/St. Paul International. [Ref. 5:p.33]

g. Closed Circuit Television Systems (CCTV)

Airports of all categories use CCTV as part of their security system. CCTV has the ability to detect and record movements of personnel entering access control areas as well as selected ingress and egress points on the airfield. [Ref. 29:p.1]

IV. ANALYSIS OF FAR 107 AND 108 AIRPORT AND AIR CARRIER EMPLOYEE ACCESS CONTROL, SCREENING, AND TRAINING REGULATIONS

This chapter is a comparison of the current Federal Aviation Regulation (FAR) 107 and 108 sections pertaining to airport and air carrier employee access control, screening, and training, and the current application of these regulations in the field. Field research was conducted at two Category X airports, two Category One airports, one Category Two airport, and a site visit to one Federal Aviation Administration (FAA) regional Office of Civil Aviation Security (ACS). This consisted of approximately 35 hours interviewing airport operations, security and screening personnel. In addition, ongoing interactive communication was maintained with the FAA ACS and these airports.

The consensus gained from our research regarding the effectiveness of current U.S. aviation security policy is that it is effective in deterring hijackers. Moreover, U.S. air carriers have not experienced a single hijacking in the last five years. [Ref. 6:p.84] The U.S. has only experienced two percent of the worldwide terrorist incidents against civil aviation in the last five years. [Ref. 6:p.83] From this data it could be interpreted that the threat against U.S. civil aviation is minimal, however, it is not. An indicator of this fact is a plot uncovered by the Federal Bureau of Investigation (FBI) in 1995 that fortunately did not occur. This was the 1995 plan to place explosive devices on 12 U.S.

airliners in the Far East for which international terrorist Ramzi Yousef was convicted in 1996. Ramzi Yousef is the suspected mastermind behind the World Trade Center bombing and was convicted of bombing Philippine Airlines flight 434 in 1994. [Ref. 6:p.49]

Since the inception of FAR 107 and 108, deterrence of terrorist attacks on airports or aircraft has been focused on the passenger, however, terrorist attacks by employees are just as conceivable. The major discrepancy of the current security regulations is the absence of standards for (1) access control systems, (2) employee background checks, and (3) training of employees in Airport Security Program (ASP) policies and procedures. Our analysis covers the following topics:

A. Employee Access Control

   1. 107.14–Access Control System

   2. 107.25–Airport Identification Media

   3. 108.13–Security of Airplanes and Facilities

B. Employee Screening

   1. 107.31 and 108.33–Access investigation

   2. 107.2 and 108.4–Falsification

C. Employee Training

   1. 108.31–Employment standards for screening personnel

Through this analysis, a more detailed assessment of the effectiveness of the current form of FAR 107 and 108 can be made.

A. ACCESS CONTROL

"The strongest castle walls are not proof against a traitor within." This ancient proverb captures the significance of the analysis contained within this section. While it is the rule for passengers and some employees to pass through metal detectors and answer security questions at the air carrier's ticket counter before accessing the aircraft gate and other restricted areas of the airport, it is not the rule for all employees.

Access control systems, identification media, and security of airplanes and facilities are all fundamental elements of the system, method, and/or procedure approved in the airport operator's ASP that provides security in the Air Operations Area (AOA).

1. 107.14–Access Control System

The implementation of 107.14 produced many different access control systems nationwide as the FAA did not mandate a standard access control system in all U.S. airports. Because of this non-standardization, and the consequent reduction in accountability, problems have arisen at individual airports that inhibit proper security. [Ref. 9]

Perhaps a benefit of non-standardization is that it allows individual airports to tailor their ASP to their specific needs. Given the freedom to choose the best system for their needs, most U.S. airports choose the system that allows them to focus on facilitating greater passenger convenience and throughput, therefore resulting in better utilization of aircraft and ultimately achieving greater airport revenues. This approach is optimal for U.S. airport and air carrier profits. Although the provision of airport security is required to some degree by all U.S. airports, it is an issue that is viewed as a hindrance to business by operators, and is routinely ranked as a low priority, until an incident occurs. [Ref. 19]

One consequence of non-standardization is the problems transient air crews confront when operating through different airports in job functions that require access to controlled areas. The current regulation only requires that there be a system, method, and/or procedure to control access to controlled areas of the airport via identification media. As a result of the regulation's language requiring only "a" system, method, or procedure and not a specific one, transient air crews must carry different identification media, if authorized to acquire it, for unescorted access through the controlled areas. Otherwise, they must be escorted, which employs security personnel away from their regular duties for that time period. Frequent delays in getting to aircraft regularly occur because of restrictions on access to the same security areas at every airport, therefore resulting in delayed flights.

Other problems arise from the inability of a security employee at an access checkpoint to effectively scrutinize identification media of transient air crews if they do not possess identification media from the airport they are operating through. Due to the variety of access control systems nationwide, access checkpoint employees do not have the immediate capability of accurately identifying transient air crews. This inability to communicate between the different systems is a hindrance to proper identification of these air crews. For example, our research examined this problem at one location. An international airport that does not have a local aircraft maintenance facility frequently requires technicians to visit the airport to perform maintenance on aircraft. This technician requires access to the AOA, but does not have identification from the host airport. Due to this, the host airport grants access based upon the technician's access identification from his or her resident airport or a telephone call to that airport to verify his or her identification, if during normal business hours, or, if after hours, the call is even answered. Now say, for example, any delay in performing the maintenance results in lost revenues for every minute the effected aircraft sits idle. In this case access may be granted without close scrutiny so as to alleviate any delay. The point made in this example is that a visiting technician is allowed access to the AOA without a thorough verification of identification. [Ref. 13] This problem would be alleviated if employee access identification information was placed into a secure, standard, non-proprietary system with an accessible data base.

Section 107.14 mandates limiting employee access to controlled areas by time and date. During interviews, employees expressed concern about the burden placed on them to meet this requirement, specifically, full compliance made it very difficult for them to accomplish their daily duties. For example, a large majority of employees work overtime and require access to facilities at irregular times and days, by limiting their access by time and date, airport operations are subject to disruption. [Ref. 9] Other factors considered in meeting this requirement are fluctuating aircraft schedules and employees filling in for other absent coworkers. Most airports use this requirement for contingency purposes, when only the strictest security measures need to be implemented.

The issuance of temporary access media to individuals who are not in possession of their original access media is a regular practice at airports. [Ref. 10] A typical example of this is an airport employee who shows up for work without his or her approved access medium and cannot practicably be escorted the entire duration of their assigned shift. Therefore, temporary access is granted based upon their current employment status. The existing regulation does not address this situation, but such temporary access media have been generally prohibited by local FAA guidance. Some airports require the individual to locate their media before allowing access while others issue a second access medium to an individual as long as access authorization is verified, and other specific standards are met.

Escort procedures for persons not in possession of access media are not specified by the regulation. Many airport operators already have some type of escort procedure in place based on FAA policy guidance, but such procedures are applied inconsistently. To ensure a more consistent application of these procedures, the FAA believes escorting standards should be incorporated into this regulation. [Ref. 11]

This regulation does not address the issue of group access to controlled areas. The airport inspections that were prompted by the Department Of Transportation (DOT) office of Inspector General (IG) audit in 1993 revealed that, despite best efforts, there are certain instances where validation of access authority has become operationally unfeasible. [Ref. 4:p.5] An access control system that validates an individual's access authorization is currently required, however, unauthorized group access, commonly known as "piggybacking", often occurs. In such an instance, more than one individual with assumed authorized access passes through an access point using only a single employees' access media, without being subject to any control measures that individually validate authorization.

Our research indicates that the only ways to effectively counter this occurrence is to execute one or more of the following: (1) place a guard at each access point to authenticate single-employee access, (2) install a revolving security door at an access point that limits only one person through at a time, or (3) in the case of vehicle access, require positive identification of all vehicle occupants and deny all unauthorized occupant's access. [Ref. 9] Our research also indicates that one more method is used instead of or in conjunction with the above. Some airports impose incentives in the form of fines and suspensions to employees that are caught piggybacking. For example, LAX revokes the employee's identification media for the first incident and makes their previous employer re-submit the proper forms, then makes them pay 75 dollars to re-acquire their media. The second incident results in the same, coupled with a suspension of 5 work days. The third incident results in termination. [Ref. 10]

As explained, the implementation of 107.14 resulted in many different airport access control systems nationwide. A plan for a national access control system, or "Universal Access System" (UAS), that would permit transient air crews to carry a single access control medium which will work at all U.S. airports, is currently under exploration by the FAA. In October 1993, Congress appropriated 2 million dollars for development and testing of this UAS to alleviate the problems associated with the current access control system. The FAA has used these funds to develop preliminary standards and functional requirements, and to field test prototype installations. [Ref. 10] However, the results of these field tests are yet to be unveiled.

While there is a general recognition that a UAS can be a good management information tool, there is no consensus on how much security is enhanced by such a system. Even with a sophisticated access control system, security will still depend on human factors and the procedures for issue and return of employee access cards. How the UAS will be paid for is another major issue to consider. Possibly a better approach, to satisfy current needs, would mandate control of access by all employees, combined with stricter FAA enforcement. Meanwhile, a UAS could be tested, debugged, and refined at selected airports. [Ref 9]

Airport operators have strongly recommended that the FAA develop technical specifications for access control systems. This recommendation also was supported by the General Accounting Office (GAO). [Ref. 7:p.12] Accordingly, the FAA agrees that there is a need for technical standards and is supporting current efforts to develop them, but does not consider section 107.14 the proper venue to issue technical standards. [Ref. 11]

2. 107.25–Airport Identification Media

Most U.S. airports use an airport identification media system of some type to satisfy the current movement control requirements of 107.14. However, there was not a specific regulatory requirement to have a system until 19 September 1991 when section 107.25 amended FAR 107, thus providing the requirement to implement this system in the U.S. Although this section does provide guidance, it is very broad and non-specific which creates some problems. Due to these problems, employee movements in secure areas can not be properly accounted for.

Section 107.25 directs employees to display an airport-approved identification media on their outermost garment at all times when operating in the Security Identification Display Area (SIDA). All U.S. airports independently determine which areas are SIDA without FAA consultation. Consequently, while some airports define the entire AOA as the SIDA, others may only define certain areas in the airport SIDA. This creates problems for security personnel in that other employees, or anyone for that matter, may enter and exit non–SIDA controlled areas of the airport without identification. [Ref. 13]

Our research indicates that problems result from the failure to direct airports to use media that displays accurate information about the individual, bears an expiration date, and indicates the individual's level of authorization for access and movement. [Ref. 13] Further, it institutes broad parameters rather than specific sizes, colors, or actual wording that must appear on the media. It also does not provide flexibility to the airports to accommodate technological advances in media.

Accountability requirements for media are also not included in this regulation. Accountability requirements ensure the integrity of a system by establishing a periodic audit and offering media revalidation or reissuance procedures. When there is no accountability for identification media, the credibility of the system is undermined. Employees are not required by the regulations (but may be required at individual airports) to return expired identification media. Security employees are also not required to safeguard unissued identification media stock and supplies. Many airports have automated identification systems that conduct audits on a scheduled basis. However, research indicates that some airports may not accomplish audits regularly, and when conducted, only after extended periods of time. [Ref. 13]

The FAA views identification systems as one of the most effective means to control movement in any portion of the AOA. [Ref. 11] Consequently, the FAA periodically audits some airports to ensure the integrity of an airport's identification system. The FAA requires airports, via written or verbal notice, to conduct a self revalidation of its system if 5 percent of identification media is determined unaccountable. Many airport operators, however, have complained that this 5 percent requirement requires revalidation or reissuance of media too frequently and does not account for the operational reality that employees will lose or misplace identification. Additionally, this may impose serious economic implications and time delays in getting the new media to employees depending on the size and operational capacity of the airport. [Ref. 9]

Finally, section 107.25 does not require an airport operator to develop a challenge program. Some airports establish their own challenge procedures to accommodate this necessity. However, a consequence of this is that standardized challenge procedures do not exist between airports. This has resulted in inconsistent challenge procedures among employees at a given airport, as well as transient air crews who perform their duties at different airports. As a result, the effectiveness of a fundamental element of the airport security program is eroded.

3. 108.13–Security of Airplanes and Facilities

Section 107.13 is concerned with AOA Security by directing air carriers to prohibit free access to airplanes and facilities. The security of air carrier operations areas is critical to assuring complete AOA security. If these areas are not secured to the same level as all other areas within the AOA, the airport is left vulnerable. However, section 108.13 does not address this issue.

It is important to note that although the title of section 108.13 includes "facilities", it does not specifically address security of facilities in its language. Additionally, it specifies "airplanes", which does not include rotorcraft or dirigibles by definition.

There currently exists little control over those having access to aircraft. For example, caterers are allowed access to the aircraft with few, if any, security checks.

Cleaning crews also enter aircraft without having their equipment, such as buckets and vacuum cleaners, screened or examined. Although this section does provide guidance, it is broad, non-specific and, as a result, leaves airplanes and facilities open to exploitation.

While procedures may exist at airports that require employees to challenge anyone not wearing proper identification in the SIDA, these procedures can be of limited effectiveness unless properly enforced. Various methods to encourage more vigorous challenging have been adopted by some airports, including a reward paid to employees for challenging unauthorized persons and turning them over to security personnel. [Ref. 9]

Under this section of FAR 108, the air carrier operator is required to *prohibit* unauthorized access to its airplanes, to check baggage and cargo, and conduct a pre-flight security inspection of the airplane. However, it does not require the air carrier to *prevent* access by unauthorized persons to baggage or cargo transported aboard a passenger aircraft. Since "prohibit" may be interpreted as only requiring placards or warnings on entrances to the air carrier's operating areas, the air carrier can circumvent proper security measures in order to maintain passenger throughput.

Our research provides information that further amplifies this point. Entry was gained into the AOA of an airport, specifically the air carrier operating areas and baggage handling facilities, by accompanying a security employee wearing identification media. Once inside these areas, it was noted that challenge to persons not wearing identification media was virtually nonexistent. Additionally, the ability to access any part of the airplane or baggage handling facility was easily accomplished, and went unnoticed by all but one employee on his lunch break. When challenged, the security employee informed the employee that we were being escorted and we then continued on our way. [Ref. 13] It is important to note that we were not wearing any type of escort access media, and challenge took place long after we had entered the area.

Lastly, section 108.13 does not require air carriers to comply with the vehicle identification procedures contained in the airport operator's ASP. This is perhaps the most egregious error in this section. Vehicle access and identification procedures are essential to mitigating risk of a major incident in the AOA due to the capacity and concealability they provide a terrorist and their weapons.

B. EMPLOYEE SCREENING

As of 1991, one in every 15 people employed in the U.S. owed his or her job to civil aviation. Of these 15 million, there are approximately 2.3 million airport and air carrier employees supporting 5,474 public facilities enplaning approximately 1.6 million passengers on a daily basis. Of these 2.3 million employees, a vast majority work in, or have access to, designated security areas on a daily basis. [Ref. 20:p.1] Prior to 26 November 1985, none of these employees were required by FAA to have employment background checks. [Ref. 2:p.43] The regulations do now require background checks, however, our research indicates that the effectiveness of these checks is debatable.

1. 107.31 and 108.33–Access Investigation

The current FAA regulations stipulate that all individuals seeking employment at airport facilities, whether employed with the airport, air carrier, or vender and requiring unescorted access into the SIDA, must undergo and pass a security background check. As written, background checks must cover the past 10 ten years of employment history and verification of the 5 preceding years commencing on the date of the investigation. The purpose of this check is to identify breaks in employment during the preceding 5 year period, which could indicate criminal history during that period. A noted 12 month gap in employment history requires the potential employer to conduct a thorough FBI background investigation.

Our research revealed that this check consists of an informal telephone verification of employment, usually conducted by a private security firm contracted to call the applicant's previous employer(s) as appearing on the job application. [Ref. 17:p.4] To avoid detection, applicants with criminal histories need only reference associates as past employers that could substantiate false employment. This method appears to be inadequate in that it provides a lesser level of scrutiny than that needed to properly screen a potential employee. Furthermore, potential employers strongly defend current procedures, insisting that this check is adequate and is in full compliance with FAA requirements.

Another problematic issue not considered in employment verification is criminal work release. Convicted criminals serving less than one year behind bars are able to bypass the 12 month gap in employment and hide their crime from this background verification. This issue provides a breach in security, thereby failing to adequately provide assurances that personnel with access to the AOA fully qualify for such access.

A probable solution to the deficiencies in employment validation and elimination of loophole issues is through the use of a secure, accurate screening system. One such system is the FBI's National Crime Information Center (NCIC) located at the Criminal Justice Information Services Division (CJIS). This system is used by the FBI to access secure intelligence databases necessary to perform organic criminal background and fingerprinting checks. These checks are highly regarded by some political entities but considered controversial by others. The Gore Commission suggests that criminal background checks are a vital security tool and have recommended FBI background and fingerprint checks for all employees with access to secure areas. [Ref. 1:p.24] Congress, via passage of the 1990 Aviation Security Improvement Act advocates FBI criminal history checks as did the Bush Commission. However, FBI criminal background checks have yet to be instituted. Airport law enforcement and airport administrators interviewed unanimously agreed that FBI checks are necessary but were in disagreement as to how to conduct this in a timely and cost effective manner.

In sharp contrast to advocates' opinions, the American Civil Liberties Union (ACLU) believes criminal background checks are problematic. The ACLU believes that the accessibility of a new government database containing personal information about employees would be an enormous risk to privacy. Moreover, the ACLU believes that the creation and maintenance of such a dynamic data base is prone to inaccuracies leading to violations of the constitutional rights of innocent employees. [Ref. 21:p.149] The airline industry believes that criminal background checks are too costly (24 dollars per check), too time consuming (up to 120 days), and that the terrorist threat is not imminent. [Ref. 22:p.5]

Based upon our research, the current system in use nationwide appears ineffective and easily defeated. It is our opinion that this system should be redesigned or eliminated and a new system put in place. In the interim, the FBI NCRC should be utilized as it is linked to federal agencies across the country including FAA and U.S. Customs offices, both located in domestic and international airports nationwide. The NCRC could be made available to the Airports' Security Coordinator (ASC) to conduct proper background checks. Though not all airports currently have direct links to this system, secure internet access is plausible making this a non-issue. Physical security of NCRC links is a fundamental concern that could be easily remedied by placing a secure terminal in a secure location accessible only by an FBI cleared ASC.

2. 107.2 and 108.4–Falsification

Falsification is an "after the fact phenomena" uncovered primarily through unrelated investigations such as those performed by Immigration Naturalization Service (INS), Drug Enforcement Agency (DEA), FAA or the local police force. Our research validated this statement as four of the five airports interviewed admitted to having first hand knowledge of on-site falsification uncovered through investigation performed by one or more of these agencies. For example, an airport operator employment investigation conducted by the INS in 1995 uncovered 112 illegal aliens cleaning terminals and aircraft at a Category One airport. All illegal aliens possessed SIDA media gained through falsified documents submitted by their employer. [Ref. 26:p.1] Though not all cases are as noteworthy as the this one, the potential for falsification exists and evidence suggests it can be found at U.S. airports.

Until recently the FAA has appeared to be a legal "toothless tiger" rarely rendering substantial penalties for such activity. In 1996 the FAA adopted sections 107.2 and 108.4 to prohibit fraudulent or intentional false statements in certain security records. As a result, they now have the ability to take legal enforcement action against individuals for falsification.

C. EMPLOYEE TRAINING

The performance and effectiveness of technology at U.S. airports today is linked directly to the quality and training of human resources. Considerable emphasis must be placed on recruitment, training, and compensation of these resources in order to provide a secure industry. It is a common practice for airports and airlines to put their trust in accessories such as metal detectors and X ray machines costing millions of dollars and to spend little on the personnel that operate them. [Ref. 23:p.85] Our research indicates that U.S. airports and air carriers routinely place the decision as to whether or not a plane is secure in the hands of poorly trained, underpaid, unmotivated, and overworked employees. [Ref. 23:p.85] Evidence of this was observed and verified at all five researched airports.

1. 108.31–Employment Standards For Screening Personnel

The only qualifications that the federal government has set for screeners is that they be able to see, hear, distinguish colors and speak and read English. [Ref. 24:p.4] Screener demographics reflect these minimum requirements as the work force is mostly made up of entry level adolescents, immigrants, and retired or future law enforcement personnel [Ref. 25:p.1] Turnover rates of between 200 to 400 percent are the norm and are directly attributed to many factors, with minimum wage compensation without insurance benefits in the forefront.

One reason for the low wages is the fierce competition for low bid contracted security firms which keeps employee compensation low. Specifically, to stay competitive, some security firms accept a high turnover rate as a trade off to paying substantially higher hourly wages such as are required by more experienced senior level screeners. As a result, the screening employee work force is understaffed, under trained, and highly ineffective when compared to the highly paid, highly trained professional screeners in Europe. Low pay increases the probability that screeners will engage in criminal activity to supplement their incomes. An example of this is a recent arrest and indictment of the security supervisor for LAX for allowing several kilos of cocaine to routinely pass through security checkpoints in return for compensation from drug traffickers. [Ref. 27:p.1]

Federal training standards for employment is a very basic 12 hour training course with 40 hours of On Job Training (OJT). Beyond setting the core requirements and guidance for initial, recurrent, and OJT, the FAA allows air carriers, through contracted security agencies, to design and implement training programs. This has resulted in a conglomeration of training programs nationwide that vary not only among air carriers, but also within air carriers. Furthermore, a survey of eight major air carriers completed by the Bush Commission indicated that, though all had specialized training curricula for detection of explosive devices and materials, a standard for this specialized training was non-existent. [Ref. 2:p.55]

Screeners are evaluated annually by local Airport Security Coordinators (ASC) and by the FAA through unannounced inspections. However, FAA inspection checklists deliberately make routine screening inspections easy to pass, by allowing only one of seven kinds of fake weapons to be placed in an uncluttered bag, on the premise that a high rate of failure would show that the airport and security system were in serious trouble. [Ref. 24:p.2] Inspection pass rates for screeners average around 90 percent, thereby giving the appearance that the current screening system is successful in detecting prohibited items. However, when inspections were done using special undercover inspection teams that are not bound to using regular checklists or test weapons, pass rates dropped to as low as 20 percent. [Ref. 24:p.2] Moreover, FAA inspection checklists have not been changed since the inception of FAR 107 and 108.

Another type of screener is the air carrier's ticket agent. The FAA places no specific standard requirement on ticket agents other than the required pre-employment access investigations and SIDA training. However, the FAA mandates verbal screening of all domestic and international passengers on baggage packing, baggage ownership, and baggage security by ticket agents. [Ref. 23:p.88] Without specialized training to perform this task effectively, it appears that ticket agents are ill prepared and ineffective in detecting passengers requiring heightened scrutiny. It can be assumed that without specialized training the possibility of a breach is heightened especially when dealing with cantankerous travelers who have been standing in long lines and are eager to be processed and allowed access to their flight. Under these conditions, ticket agents can be expected to respond by reducing thorough screening in order to maximize passenger throughput.

An example of an effective screening system is utilized by El Al Airlines of Israel. Unlike the U.S. and Europe, El Al devotes highly specialized security agents specifically to screening passengers, thus allowing ticket agents to concentrate on their primary task–accommodating passengers. El Al security agents are versed in identifying suggestive signs of lying, such as eye and body language. [Ref. 23:p.88]

Section 107.25 requires all persons with unescorted access to the SIDA to have training directly related to SIDA operations. Our research indicates that training is nothing more than required reading and the viewing of FAA instructional videotapes covering basic airport operations. The cumulative time for students to complete training was dependent upon individual aptitude, though it was noted that even the slowest reader could complete the training within one hour. Furthermore, our research indicates that instruction was dissimilar between airports. Instruction over and above that required by the FAA was provided at 50 percent of the visited facilities, whereas no instruction was provided at the remaining sites.

V. CORRECTIVE MEASURES

The best means to address the challenges and issues of the current and future terrorist threat to civil aviation is to revise current airport and airport operator security regulations. Based upon issues analyzed in chapter four, this chapter offers corrective measures for improving (1) Airport and Air Carrier Employee Access Control, (2) Airport and Air Carrier Employee Screening, and (3) Airport and Air Carrier Employee Training. The recommendations that follow are based on our field research of five U.S. airports and examination of the current Federal Aviation Regulations (FAR).

A. ACCESS CONTROL

1. Mandate a Standard AOA Access Control Strategy at all U.S. Airports

Success in deterring terrorist incidents within the Air Operations Area (AOA) will depend on the FAA's ability to provide technical standards for a system, method, and/or procedure to address the problem of employee accountability. Perhaps the most critical element of this system is for the FAA to mandate that all employees must pass through security screening checkpoints before accessing the aircraft gate and other restricted areas of the airport. These checkpoints must include one or more of the following: (1) placing a guard at each access point to authenticate single-employee access, (2) installing revolving security doors at access points that allows only one employee through at a time, and (3) in the case of vehicle access, requiring positive identification of all vehicle occupants.

The cost of these measures is a key decision factor for their procurement. Placing a guard at each access point incurs labor costs, and revolving doors currently cost $50,000 each. [Ref. 9] Perhaps a cost effective way for airports to afford these measures is to reduce the number of AOA access points and/or utilize Federal Aviation Administration (FAA) Airport Improvement Program (AIP) funds. The AIP is currently authorized by the FAA for use in airport capital improvement projects such as runways, roads, terminal expansion, and perimeter security fences. However, improvements to other security equipment does not qualify for these funds. [Ref. 13] The FAA should authorize these funds for use in all security improvement projects and allow airport operators flexibility in implementing the checkpoint system that best suits their needs from those listed above. This flexibility is paramount in order to minimize expense and disruptions in efficient employee work routines.

Other corrective measures include removing the requirement that limits employee access to controlled areas by time and date, implementing mandatory AOA escort procedures, making the AOA in all U.S. airports a Security Identification Display Area (SIDA) and establishment of the Universal Access System (UAS) as described in Chapter IV.

2. Mandate Standard Airport Identification Media

A standard for operator identification media is the cornerstone of an effective access control strategy. A UAS would mandate standard media as part of its structure. However, this standard should also mandate control of access media by the Airport Security Coordinator (ASC), include regular audits of issued access media, and create measures to ensure that access controls are locally enforced and cannot be used to gain unauthorized access to the SIDA of other airports. This media should also display accurate information about the individual, bear an expiration date, and indicate the individual's level of authorization for access and movement. Further, this standard should institute specific parameters for media size, color, and wording that must appear on it.

The FAA should also conduct periodic, unannounced audits of all U.S. airports to ensure the integrity of the airport identification media system and fine airports found non-compliant. These fines should be placed into the AIP and be authorized by the FAA for use in security improvement projects. Additionally, the FAA should also survey all airports and determine an efficient percentage of unaccountable media that is allowable based upon the characteristics of the airport. This is in lieu of the current five percent requirement described in Chapter IV. Finally, this standard must require airports to utilize an FAA implemented, standard challenge program.

3. Mandate the Security of Airplanes and Facilities subject to Standard AOA Access Control System Requirements

In order to implement a truly comprehensive AOA access control strategy, the FAA must require all air carrier's to screen all employees authorized entry into the AOA by making standard AOA access control standards apply to aircraft and facilities. The first essential is to redesignate the title of Federal Aviation Regulation (FAR) section 108.13 to include "aircraft" instead of "airplanes." This would legally bind air carriers to provide security for all flying vehicles under their control. The second essential element is watertight control of every means of access to the aircraft through maintenance areas, cargo sheds, kitchens, other access points from the terminal buildings, and from outside the airport. These access points should be monitored by airport security staff checking identification media, using metal and explosive detectors and, where necessary, hand search. All cargo and kitchen supplies should be similarly monitored. Vapor sniffing equipment should also be utilized to detect drugs, other contraband and explosives. Third, every employee issued identification media giving access to the AOA (engineers, cleaners, kitchen, fuel and cargo handlers, transient air crews, etc.) should have successfully passed a background security check prior to employment. Their identification media should contain data designed to prevent impersonation. Finally, particular care should be taken to confirm identification and otherwise control transient air crews. Because of their transient nature, the presence of these crews may represent a weak link in the security system for infiltration.

B. SCREENING

1. Mandate Federal Bureau of Investigation (FBI) Background and Fingerprint Checks for all Airport and Airline Employees

Failure to thoroughly screen employees having access to secure airport areas can sharply undermine the capability of an Airport Security Program (ASP) and result in disastrous consequences. Telephone verification of an employee's precursory five year employment history is ineffective, easily subverted, and has problematic loopholes. The best way to ensure the integrity of employees is for the FAA to mandate FBI background and fingerprint checks for all employees. The following steps can be taken by the FAA in this regard:

1. Utilize the FBI's National Crime Information Center (NCIC) 2000 system at Category X, One, Two and Three airports to perform background and fingerprint checks. Solicit the FBI to provide training and certification for both FAA personnel and ASC's on this system. Once certified, ASC's will be primarily responsible for performing all checks with the FAA maintaining responsibility for system oversight.
2. Institute new standards for background investigations. Standards should consider ACLU concerns while providing clear concise policy and procedures.
3. Prioritize checks so that new hires are scrutinized first. Current employees should be temporarily grandfathered to avoid extensive backlogs and system overload. All employees should be screened within a 2 year period.

2. Prosecute all Entities Engaged in Falsification of Security Records

A chain is only as strong as its weakest link. Falsification is the link most likely to cause failure of a well developed security chain. The FAA must make public examples of all engaged in such activities by prosecuting and heavily fining them according to the violation and place fines into the AIP. Stiff financial penalties, incarceration, and/or industry humiliation should deter such activities.

3. Require Airlines to Hire Professional Passenger Screening Personnel

The practice of using ticket agents as a front line of defense in screening passengers is ineffective. Adopting El Al Airline's practice of hiring only highly trained security agents that are well versed in identifying signs of deception can greatly enhance security. The ticket agent's job is to assist in getting passengers their scheduled flight, not keep them off. [Ref. 23:p.88] Although this measure may increase labor costs, and would most likely disproportionately impact smaller, less prosperous airports, it is yet another measure that could be funded by the Airport Improvement Program (AIP).

C. TRAINING

1. Intensify Employment Standards and Employee Training

The FAA has failed to provide adequate baseline requirements and standards for both employee hiring and training. As a result, security is placed in the hands of underpaid, untrained, unmotivated, and overworked workforce who are given little incentive to feel good about themselves or their jobs. Turnover rates in these jobs are currently at epidemic 200 to 400 percent, and minimum wage pay may create an incentive for some employees to engage in criminal activities to supplement their income. Some industry officials feel that training and skill levels are so poor that efforts to implement new Explosive Detection System (EDS) technologies are being held back. [Ref. 24:p.3]

In light of these factors, the FAA should mandate measures which accomplish the following objectives and thereby establish a more effective employment and training system:

1. Raise the quality of security personnel by choosing bright, educated people; training them well; testing them frequently; and paying them a decent wage. At $5.60 an hour, you get what you pay for.
2. Develop universal performance standards for selection, training, certification and recertification of screening companies and their employers. [Ref. 1:p.28]
3. Deploy state of the art computerized training and testing systems. One such current system, called "SPEARS," projects computer generated images of hundreds of different kinds of weapons carried inside passenger luggage on a screener's X ray monitor.

As previously mentioned, the AIP could be used to fund these measures.

2. Revise FAA Security Inspection Rules and Practices to Realistically Assess the Security System and Provide Employee Training

Inspection rules and practices developed in the 1970's must be updated to 1990's standards. The FAA's Civil Aviation Security (ACS) agents must create and utilize a revised and realistic airport security inspection checklist so as to fully test the security system. The current checklist is inadequate in that it deliberately makes routine screening inspections easy to pass, and only allows one of seven different types of imitation weapons to be used in inspections.

Our research found that the FAA makes airport security inspections easy to pass so that, statistically, the airport and the FAA appear successful in the provision of an effective security system. The FAA maintains that the current inspection criteria and security system adequately address the threat. However, by allowing easy inspections, the credibility of the system is undermined. The employees being inspected do not currently receive training from the FAA in conjunction with the inspection. In order to create effective airport security inspection procedure, the FAA needs to provide a number of cyclical, scheduled assist visits to airports and provide training to employees in the proper security procedures and regulations. The FAA should complete the training cycle by conducting an inspection and fining employees and operators for discrepancies. These fines would then be placed into the AIP. Fining employees and operators establishes an incentive to properly provide security at our nations' airports.

VI. CONCLUSIONS AND RECOMMENDATIONS

The number of civil aviation incidents worldwide has dropped by nearly two thirds from 1992 to 1996. [Ref. 6:p.50] This, however, has not translated into a corresponding decline in the threat to U.S. civil aviation interests, as indicated in Chapter II. There is every reason to believe that civil aviation will continue to be an attractive target for terrorist groups. This threat will remain significant in the foreseeable future, and the fact that some years pass with fewer incidents does not necessarily indicate that the threat has diminished.

The U.S. has enjoyed a benign history of persistent terrorist incidents. However, threats initiating from Middle East adversaries in response to our military and foreign policies, the destruction of the Oklahoma City Federal Building, and the bombing of the New York city World Trade Center all suggest that threats persist and can be catastrophic. Success in deterring threats to the civil aviation industry rests upon revision of the FAA airport and airport operator security regulations analyzed in this thesis to adequately address this issue.

This last chapter is presented in three sections. The first section describes the current state of employee-related security as determined by our examination of the regulations and field research at five U.S. airports. Solutions for these problems are provided in the second section. The first two sections recapitulate material respectively presented in Chapters IV and V. The third section provides a brief close to this thesis.

A. CONCLUSIONS

1. Access Control

a. A Standard Air Operations Area (AOA) Access Control Strategy does not exist at all U.S. Airports

The implementation of 107.14 produced many different access control systems nationwide as the FAA did not mandate a standard access control system in all U.S. airports. Due to this, integration of the myriad of access control systems nationwide is impossible. Among other consequences, airports are not able to access information on transient personnel and adequately scrutinize their identity.

As indicated in Chapter IV, a benefit of non-standardization is that most U.S. airports are able to choose the system that allows them to focus on facilitating greater passenger convenience and throughput, therefore resulting in better utilization of aircraft and ultimately achieving greater airport revenues. However, consequences of non–standardization outweigh the benefits. Non-standardization does not effectively offer the U.S. air travel industry the consistent level of protection needed to counter modern terrorism but rather offers the terrorist windows of opportunity to engage their tactics.

b. Standard Airport Identification Media is not Utilized

Problems result from the failure to direct airports to use media that displays accurate information about the individual, bears an expiration date, and indicates the individual's level of authorization for access and movement. [Ref. 13] Further, the current regulations institute broad parameters rather than specific sizes, colors, or actual wording that must appear on the media. It also does not provide flexibility to the airports to accommodate technological advances in media.

Accountability requirements for media are also not included in this regulation. Accountability requirements ensure the integrity of a system by establishing a periodic audit and offering media revalidation or reissuance procedures. Employees are not required by the regulations, (but may be required at individual airports), to return expired identification media. Security employees are also not required to safeguard unissued identification media stock and supplies. Some airports may not accomplish audits regularly, and when conducted, only after extended periods of time. [Ref. 13] Additionally, standardized challenge procedures do not exist between airports. This has resulted in inconsistent challenge procedures among employees at a given airport, as well as with transient air crews who perform their duties at different airports.

c. The Security of Airplanes and Facilities is not subject to Standard AOA Access Control System Requirements

Under this section of FAR 108, the air carrier operator is required to *prohibit* unauthorized access to its airplanes, to check baggage and cargo, and conduct a pre-flight security inspection of the airplane. However, it does not require the air carrier to *prevent* access by unauthorized persons to baggage or cargo transported aboard a passenger aircraft. "Prohibit" may be interpreted as only placing placards or warnings on entrances to the air carrier's operating areas, so that the air carrier can circumvent proper security measures in order to maintain passenger throughput.

2. SCREENING

a. Federal Bureau of Investigation Background and Fingerprint Checks for Airport and Airline Employees are not Required

Pre employment screening for individuals seeking positions with unescorted access to high level airport security areas is less than that required for employment in a bank or child care center. FAA regulations mandate nothing more than documentation of an applicant's past 10 year employment history. Accurate information on an applicant based upon this time period is sometimes difficult to acquire or is falsified. Therefore, individuals with questionable backgrounds may attain employment and unimpeded access to airport facilities and aircraft.

Federal Bureau of Investigation (FBI) background and fingerprint checks have yet to be mandated by the FAA. This is mainly due to strong opposition by the American Civil Liberties Union (ACLU) and the airline industry.

b. Falsification of Security Records is Problematic

Falsification of security documentation is a common occurrence and has led to serious breeches of airport security areas. Four of five airports interviewed identified cases of falsification at their facilities uncovered by federal and local police agencies performing investigations unrelated to employment. Falsification is a universal activity performed not only by employees but unscrupulous employers seeking to minimize manpower costs as noted in Chapter IV. The security of air travelers cannot be assured until the integrity of our nation's aviation workforce is certain.

c. Ticket Agents are Ill Prepared to Screen Passengers

FAA mandates requiring air carriers to perform verbal passenger screening is delegated to ticket agents who have neither the formal training or practical experience to perform such. Ticket agents are ill prepared to effectively scrutinize passengers and identify suggestive signs of lying, such as eye contact and body language. When agents are confronted with long lines of irritable passengers they often tend to concentrate on maximization of throughput at the expense of thorough verbal screening.

3. TRAINING

a. Employee Standards and Training are Questionable

The only qualifications that the federal government has set for screeners is that they be able to see, hear, distinguish colors and speak and read English. [Ref 24:p.4]. Screener demographics reflect these minimum requirements as the workforce is made up of entry level adolescents, immigrants, and retired law enforcement personnel, all of which contribute to a 200 to 400 percent annual turnover rate nationwide. Training requirements mandated by FAA are nothing more than a very basic 12 hour training course with 40 hours of on the job training. As a result screener inspection pass rates have dropped as low as 20 percent at some facilities inspected by undercover FAA inspectors.

b. FAA Inspection Rules and Practices are Ineffective and Outdated

Inspection rules and practices have not been substantially changed or modified since the inception of FAR 107 and 108. Current FAA inspection checklist criteria deliberately makes routine screening inspections easy to pass, by allowing only one of seven kinds of fake weapons to be placed in an uncluttered bag. [Ref. 24:p. 2] Additionally, the employees being inspected do not currently receive training from the FAA in conjunction with the inspection. The FAA maintains that the current inspection criteria and security system adequately address the threat. However, this position is questionable.

B. RECOMMENDATIONS

Success in deterring threats to the civil aviation industry rests upon revision of the FAA airport and airport operator security regulations analyzed in this thesis. Without question, the U.S. civil aviation industry needs revised security regulations to adequately counter the threat of terrorism.

Based upon issues explored previously, this section offers recommendations for improving: (1) Airport and Air Carrier Employee Access Control, (2) Airport and Air Carrier Employee Screening, and (3) Airport and Air Carrier Employee Training.

1. Access Control

a. Mandate a Standard Air Operations Area (AOA) Access Control Strategy at all U.S. Airports

The FAA should mandate and subsidize implementation of the Universal Access System" (UAS) and mandate that all employees must pass through security screening checkpoints before accessing the aircraft gate and other restricted areas of the airport. These checkpoints must include one or more of the following: (1) placing a guard at each access point to authenticate single-employee access, (2) installing revolving security doors at access points that allows only one employee through at a time, and (3) in the case of vehicle access, require positive identification of all vehicle occupants.

Additionally, the FAA should remove the requirement that limits employee access to controlled areas by time and date, implement mandatory AOA escort procedures, and make the AOA in all U.S. airports a Security Identification Display Area (SIDA).

b. Mandate Standard Airport Identification Media

A UAS would mandate standard media as part of its structure. However, this standard should also mandate control of access media by the Airport Security Coordinator (ASC), include regular audits of issued access media, and create measures to ensure that access controls are locally enforced and cannot be used to gain unauthorized access to the SIDA of other airports. This media should also display accurate information about the individual, bear an expiration date, and indicate the individual's level of authorization for access and movement. Further, this standard should institute specific parameters for media size, color, and wording that must appear on it. The FAA should also conduct periodic, unannounced audits of all U.S. airports, implement a standard challenge system, and determine the best percentage of unaccountable media allowed based upon an airport's operating characteristics.

c. Mandate the Security of Airplanes and Facilities subject to Standard AOA Access Control System Requirements

The FAA should require all air carrier's to screen all employees authorized entry into the AOA by making standard AOA access control standards apply to aircraft and facilities. The FAA should redesignate the title of Federal Aviation Regulation (FAR) section 108.13 to include "aircraft" instead of "airplanes," and maintain watertight control of every means of access to the aircraft through maintenance areas, cargo sheds, kitchens, other access points from the terminal buildings, and from outside the airport by staffing these areas with security employees. Finally, the FAA should mandate that every employee issued identification media giving access to the AOA, must have successfully passed a background security check prior to their employment.

2. SCREENING

a. Mandate Federal Bureau of Investigation (FBI) Background and Fingerprint Checks for all Airport and Airline Employees

Telephone verification of an employee's precursory five year employment history is ineffective, easily subverted, and has problematic loopholes. The best way to ensure the integrity of employees is for the FAA to mandate FBI background and fingerprint checks for all employees. The FAA should: (1) utilize the FBI's National Crime Information Center (NCIC) 2000 system at Category X, One, Two and Three airports to perform background and fingerprint checks, (2) institute new standards for background investigations, and (3) prioritize checks so that new hires are scrutinized first. All employees should be screened within a 2 year period.

b. Prosecute all Falsifications of Security Records

The FAA should make public examples of all engaged in security record falsification by prosecuting and heavily fining them according to the violation. Stiff financial penalties, incarceration, and/or industry humiliation should deter such activities.

c. Require Airlines to Hire Professional Passenger Screening Personnel

The practice of using ticket agents as a front line of defense in screening passengers is ineffective. Adopting El Al Airline's practice of hiring only highly trained security agents that are well versed in identifying signs of deception can greatly enhance security.

3. TRAINING

a. Intensify Employment Standards and Employee Training

The FAA should: (1) raise the quality of security personnel through the selection process, training and testing programs, and wage levels, (2) develop universal performance standards for the selection, training, certification and recertification of screening companies and their employees, and (3) deploy state of the art computerized training and testing systems.

b. Revise FAA Security Inspection Rules and Practices to Realistically Assess the Security System and Provide Employee Training

The FAA must create and utilize a revised and realistic airport security inspection checklist so as to fully test the security system. In order to create effective airport security inspection procedure, the FAA needs to provide a number of cyclical, scheduled assist visits to airports and provide training to employees in the proper security procedures and regulations. The FAA should complete the training cycle by conducting an inspection and fining employees and operators for discrepancies.

C. SUMMARY

The FAA and U.S. airports, in particular, are the intended primary beneficiaries of this research. The FAA, and airport officials and planners may be able to apply the information gained to possibly improve the overall security of the U.S. air travel system. Through this research, a more effective practice of individual and corporate responsibility for complying with security regulations may be achieved for all U.S. Category X, One, Two, Three, Four and Five airports.

The Department Of Defense (DOD) may also benefit from these findings in managing the operations of common user air lift terminals such as Naval Air Station (NAS) Norfolk, Dover Air Force Base (AFB), and Travis AFB in peacetime and in war.

APPENDIX

This appendix provides the official FAA form of FAR 107 and 108 as provided by the U.S. Federal Register.

A. FAR 107 AND 108

1. Airport Access Control

Sec. 107.14–Access Control System.

(a) Except as provided in paragraph (b) of this section, each operator of an airport regularly serving scheduled passenger operations conducted in airplanes having a passenger seating configuration of more than 60 seats shall submit to the Director of Civil Aviation Security (ACS), for approval and inclusion in its approved security program, an amendment to provide for a system, method, or procedure which meets the requirements specified in this paragraph for controlling access to secured areas of the airport. The system, method, or procedure shall ensure that only those persons authorized to have access to secured areas by the airport operator's security program are able to obtain that access and shall specifically provide a means to ensure that such access is denied immediately at the access point or points to individuals whose authority to have access changes. The system, method, or procedure shall provide a means to differentiate between persons authorized to have access to only a particular portion of the secured areas and persons authorized to have access only to other portions or to the entire secured area. The system, method, or procedure shall be capable of limiting an individual's access by time and date.

(b) The Director of ACS will approve an amendment to an airport operator's security program that provides for the use of an alternative system, method, or procedure if, in the Director's judgment, the alternative would provide an overall level of security equal to that which would be provided by the system, method, or procedure described in paragraph (a) of this section.

(c) Each airport operator shall submit the amendment to its approved security program required by paragraph (a) or (b) of this section according to the following schedule:

(1) By August 8, 1989, or by 6 months after becoming subject to this section, whichever is later, for airports where at least 25 million persons are screened annually or airports that have been designated by the Director of Civil Aviation Security. The amendment shall specify that the system, method, or procedure must be fully operational within 18 months after the date on which an airport operator's amendment to its approved security program is approved by the Director of ACS.

(2) By August 8, 1989, or by 6 months after becoming subject to this section, whichever is later, for airports where more than 2 million persons are screened annually. The amendment shall specify that the system, method, or procedure must be fully operational within 24 months after the date on which an airport operator's amendment to its approved security program is approved by the Director of ACS.

(3) By February 8, 1990, or by 12 months after becoming subject to this section, whichever is later, for airports where at least 500,000 but not more than 2

million persons are screened annually. The amendment shall specify that the system, method, or procedure must be fully operational within 30 months after the date on which an airport operator's amendment to its approved security program is approved by the Director of ACS.

(4) By February 8, 1990, or by 12 months after becoming subject to this section, whichever is later, for airports where less than 500,000 persons are screened annually. The amendment shall specify that the system, method, or procedure must be fully operational within 30 months after the date on which an airport operator's amendment to its approved security program is approved by the Director of ACS.

(d) Notwithstanding paragraph (c) of this section, an airport operator of a newly constructed airport commencing initial operation after December 31, 1990, as an airport subject to paragraph (a) of this section, shall include as part of its original airport security program to be submitted to the FAA for approval a fully operational system, method, or procedure in accordance with this section.

Sec. 107.25–Airport identification media.

(a) As used in this section, Security Identification Display Area (SIDA) means any area identified in the airport security program as requiring each person to continuously display on their outermost garment, an airport-approved identification medium unless under airport-approved escort.

(b) After January 1, 1992, an airport operator may not issue to any person any identification media that provides unescorted access to any security identification display area unless the person has successfully completed training in accordance with an FAA-approved curriculum specified in the security program.

(c) By October 1, 1992, not less than 50 percent of all individuals possessing airport-issued identification that provides unescorted access to any security identification display area at that airport shall have been trained in accordance with an FAA-approved curriculum specified in the security program.

(d) After May 1, 1993, an airport operator may not permit any person to possess any airport-issued identification medium that provides unescorted access to any security identification display area at that airport unless the person has successfully completed FAA-approved training in accordance with a curriculum specified in the security program.

(e) The curriculum specified in the security program shall detail the methods of instruction, provide attendees the opportunity to ask questions, and include at least the following topics:

(1) Control, use, and display of airport-approved identification or access media.

(2) Challenge procedures and the law enforcement response which supports the challenge procedure.

(3) Restrictions on divulging information concerning an act of unlawful interference with civil aviation if such information is likely to jeopardize the safety of domestic or international aviation.

(4) Non-disclosure of information regarding the airport security system or any airport tenant's security systems.

(5) Any other topics deemed necessary by the Assistant Administrator for ACS.

(f) No person may use any airport-approved identification medium that provides unescorted access to any security identification display area to gain such access unless that medium was issued to that person by the appropriate airport authority or other entity whose identification is approved by the airport operator.

(g) The airport operator shall maintain a record of all training given to each person under this section until 180 days after the termination of that person's unescorted access privileges.

Sec. 108.13–Security of airplanes and facilities.

Each certificate holder required to conduct screening under a security program shall use the procedures included, and the facilities and equipment described, in its approved security program to perform the following control functions with respect to each airplane operation for which screening is required:

(a) Prohibit unauthorized access to the airplane.

(b) Ensure that baggage carried in the airplane is checked in by a responsible agent and that identification is obtained from persons, other than known shippers, shipping goods or cargo aboard the airplane.

(c) Ensure that cargo and checked baggage carried aboard the airplane is handled in a manner that prohibits unauthorized access.

(d) Conduct a security inspection of the airplane before placing it in service and after it has been left unattended.

2. Operator Screening

Sec. 107.2 and 108.4–Falsification.

No person may make, or cause to be made, any of the following:

(a) Any fraudulent or intentionally false statement in any application for any security program, access medium, or identification medium, or any amendment thereto, under this part.

(b) Any fraudulent or intentionally false entry in any record or report that is kept, made, or used to show compliance with this part, or exercise any privileges under this part.

(c) Any reproduction or alteration, for fraudulent purpose, of any report, record, security program, access medium, or identification medium issued under this part.

Sec. 107.31 and 108.33–Access Investigation.

(a) On or after January 31, 1996, this section applies to all individuals seeking authorization for, or seeking authority to authorize others to have, unescorted access privileges to the SIDA that is identified in the airport security program as defined by Sec. 107.25.

(b) Except as provided in paragraph (e) of this section, each airport operator must ensure that no individual is granted authorization for, or is granted authority to authorize others to have, unescorted access to the area identified in paragraph (a) of this section unless:

(1) The individual has satisfactorily undergone a review covering the past 10 years of employment history and verification of the 5 years preceding the date the access investigation is initiated as provided in paragraph (c) of this section.

(2) The results of the access investigation do not disclose that the individual has been convicted or found not guilty by reason of insanity, in any jurisdiction, during the 10 years ending on the date of such investigation, of a crime involving any of the following crimes enumerated in paragraphs (b)(2)(i) through (xxv) of this section. Where specific citations are listed, both the current citation and the citation that applied before the statutes are recodified in 1994 are listed.

(i) Forgery of certificates, false making of aircraft, and other aircraft registration violations, 49 U.S.C. 46306 [formerly 49 U.S.C. App. 1472 (b)].

(ii) Interference with air navigation, 49 U.S.C. 46308, [formerly 49 U.S.C. App 1472 (c)].

(iii) Improper transportation of a hazardous material, 49 U.S.C. 46312, formerly 49 U.S.C. App 1472(b)(2)].

(iv) Aircraft piracy, 49 U.S.C. 46502, [formerly 49 U.S.C. App 1472(i).

(v) Interference with flightcrew members or flight attendants, 49 U.S.C. 46504, [formerly 49 U.S.C. App 1472(j)].

(vi) Commission of certain crimes aboard aircraft in flight, 49 U.S.C. 46506, [formerly 49 U.S.C. App 1472(k)].

(vii) Carrying a weapon or explosive aboard an aircraft, 49 U.S.C. 46505 [formerly 49 U.S.C. App 1472(l)].

(viii) Conveying false information and threats, 49 U.S.C. 49 46507 [formerly 49 U.S.C. App 1472 (m)].

(ix) Aircraft piracy outside the special aircraft jurisdiction of the United States, 49 U.S.C. 46502(b), [formerly 49 U.S.C. App 1472(n)].

(x) Lighting violations involving transporting controlled substances, 49 U.S.C. 46315, [formerly 49 U.S.C. App 1472(q)].

(xi) Unlawful entry into an aircraft or airport area that serves air carriers or foreign air carriers contrary to established security requirements, 49 U.S.C. 46314, [formerly 49 U.S.C. App 1472(r)].

(xii) Destruction of an aircraft or aircraft facility, 18 U.S.C. 32.

(xiii) Murder.

(xiv) Assault with intent to murder.

(xv) Espionage.

(xvi) Sedition.

(xvii) Kidnapping or hostage taking.

(xviii) Treason.

(xix) Rape or aggravated sexual abuse.

(xx) Unlawful possession, use, sale, distribution, or manufacture of an explosive or weapon.

(xxi) Extortion.

(xxii) Armed robbery.

(xxiii) Distribution of, or intent to distribute, a controlled substance.

(xxiv) Felony arson.

(xxv) Conspiracy or attempt to commit any of the aforementioned criminal acts.

(c) The access investigation must include the following steps:

(1) The individual must complete an application form that includes:

(i) The individual's full name, including any aliases or nicknames.

(ii) The dates, names, phone numbers, and addresses of previous employers, with explanations for any gaps in employment of more than 12 months, during the previous 10-year period.

(iii) Notification that the individual will be subject to an employment history verification and possibly a criminal history records check.

(iv) Any convictions during the previous 10-year period of the crimes listed in paragraph (b)(2) of this section.

(2) The identity of the individual must be verified through the presentation of two forms of identification, one of which must bear the individual's photograph.

(3) The information on the most recent 5 years of employment history required under paragraph (c)(1)(ii) of this section must be verified in writing, by documentation, by telephone, or in person.

(4) If one or more of the following conditions exists, the access investigation must not be considered complete unless it includes a check of the individual's fingerprint-based criminal history record maintained by the FBI. The airport operator may request a check of the individual's fingerprint-based criminal history record only if one or more of the following conditions exists:

(i) The individual cannot satisfactorily account for a period of unemployment of 12 months or more during the previous 10-year period.

(ii) The individual is unable to support statements made or there are significant inconsistencies between information provided on the application in response to questions required by paragraph (c)(1)(ii) of this section and that obtained through the 5-year verification process.

(iii) Information becomes available to the airport operator during the access investigation indicating a possible conviction for one of the disqualifying crimes.

(d) An airport operator may permit an individual to be under escort as defined in Sec. 107.1 in accordance with the airport security program to the areas identified in paragraph (a) of this section.

(e) Notwithstanding the requirements of this section, an airport operator may authorize the following individuals to have unescorted access to the areas identified in paragraph (a) of this section:

(1) Employees of the Federal government or a state or local government (including law enforcement officers) who, as a condition of employment, have been subject to an employment investigation.

(2) Crew members of foreign air carriers covered by an alternate security arrangement in the approved airport operator security program.

(3) An individual who has been continuously employed in a position requiring unescorted access by another airport operator, airport tenant or air carrier.

(4) An individual who has access authority to the U.S. Customs Service security area of the U.S. airport.

(f) An airport operator will be deemed to be in compliance with its obligations under paragraphs (b)(1) and (b)(2) of this section, as applicable, when it accepts certification from:

(1) An air carrier subject to Sec. 108.33 of this chapter that the air carrier has complied with Sec. 108.33 (a)(1) and (a)(2) for its employees and contractors.

(2) An airport tenant other than a U.S. air carrier that the tenant has complied with paragraph (b)(1) of this section for its employees.

(g) The airport operator must designate the airport security coordinator to be responsible for:

(1) Reviewing and controlling the results of the access investigation.

(2) Serving as the contact to receive notification from an individual applying for unescorted access of his or her intent to seek correction of his or her criminal history record with the FBI.

(h) Prior to commencing the criminal history records check, the airport operator must notify the affected individuals.

(i) The airport operator must collect and process fingerprints in the following manner:

(1) One set of legible and classifiable fingerprints must be recorded on fingerprint cards approved by the FBI for this purpose.

(2) The fingerprints must be obtained from the individual under direct observation by the airport operator.

(3) The identity of the individual must be verified at the time fingerprints are obtained. The individual must present two forms of identification media, one of which must bear his or her photograph.

(4) The fingerprint card must be forwarded to Federal Aviation Administration, 800 Independence Ave., S.W., Washington, D.C. 20591 (ATTN: ACO-310, Access Processing).

(5) Fees for the processing of the criminal checks are due upon application. Airport operators shall submit payment through corporate check, cashier's check or money order made payable to "U.S. FAA," at the rate of $24.00 for each fingerprint card. Combined payment for multiple applications is acceptable.

(j) In conducting the criminal history records check required by this section, the airport operator must ascertain information on arrests for the crimes listed in paragraph (b)(2) of this section for which no disposition has been recorded to make a determination of the outcome of the arrest.

(k) The airport operator must:

(1) At the time the fingerprints are taken, notify the individual that a copy of any criminal history record received from the FBI will be made available if requested in writing.

(2) Prior to making a final decision to deny authorization for unescorted access, advise the individual that the FBI criminal history record discloses information that would disqualify him or her from unescorted access authorization and provide each affected individual with a copy of his or her FBI record if it has been requested. The individual may contact the local jurisdiction responsible for the information and the FBI to complete or correct the information contained in the record before any final access decision is made, subject to the following conditions:

(i) Within 30 days after being advised that the FBI criminal history record discloses disqualifying information, the individual must notify the airport operator, in writing, of his or her intent to correct any information believed to be inaccurate. If no notification is received within 30 days, the airport operator may make a final access decision.

(ii) Upon notification by the individual that a record has been corrected, the airport operator must obtain a copy of the revised FBI record prior to making a final access decision.

(3) Notify an individual that a final decision has been made to grant or deny authorization for unescorted access.

(l) Any individual authorized to have unescorted access privilege to the areas identified in paragraph (a) of this section who is subsequently convicted of any of the crimes listed in paragraph (b)(2) of this section must report the conviction and surrender the SIDA identification medium within 24 hours to the issuer.

(m) Criminal history record information provided by the FBI must be used solely for the purposes of this section, and no person shall disseminate the results of a criminal history records check to anyone other than:

(1) The individual to whom the record pertains or that individual's authorized representative.

(2) The airport operator.

(3) Others designated by the Administrator.

(n) The airport must maintain a written record for each individual until 180 days after the termination of the individual's authority for unescorted access. The records for each individual subject to:

(1) The access investigation must include: the application, the employment verification information obtained by the employer, the names of those from whom the employment verification information was obtained, the date the contact was made, or certification of same from air carriers of airport tenants, and any other information as required by the Assistant Administrator for ACS.

(2) A criminal history records check must include the results of the records check, or a certification by the airport operator or air carrier

that the check was completed and did not uncover a disqualifying conviction. These records must be maintained in a manner that protects the confidentiality of the employee, which is acceptable to the Assistant Administrator for ACS.

3. Operator Training

Sec. 108.31–Employment standards for screening personnel.

(a) No certificate holder shall use any person to perform any screening function, unless that person has:

(1) A high school diploma, a General Equivalency Diploma, or a combination of education and experience which the certificate holder has determined to have equipped the person to perform the duties of the position.

(2) Basic aptitudes and physical abilities including color perception, visual and aural acuity, physical coordination, and motor skills to the following standards:

(i) Screeners operating X-ray equipment must be able to distinguish on the X-ray monitor the appropriate imaging standard specified in the certificate holder's security program. Wherever the X-ray system displays colors, the operator must be able to perceive each color.

(ii) Screeners operating any screening equipment must be able to distinguish each color displayed on every type of screening equipment and explain what each color signifies.

(iii) Screeners must be able to hear and respond to the spoken voice and to audible alarms generated by screening equipment in an active checkpoint environment.

(iv) Screeners performing physical searches or other related operations must be able to efficiently and thoroughly manipulate and handle such baggage, containers, and other objects subject to security processing.

(v) Screeners who perform pat-downs or hand-held metal detector searches of persons must have sufficient dexterity and capability to conduct those procedures on all parts of the persons' bodies.

(3) The ability to read, speak, and write English well enough to:

(i) Carry out written and oral instructions regarding the proper performance of screening duties.

(ii) Read English language identification media, credentials, airline tickets, and labels on items normally encountered in the screening process.

(iii) Provide direction to and understand and answer questions from English-speaking persons undergoing screening.

(iv) Write incident reports and statements and log entries into security records in the English language.

(4) Satisfactorily completed all initial, recurrent, and appropriate specialized training required by the certificate holder's security program.

(b) Notwithstanding the provisions of paragraph (a)(4) of this section, the certificate holder may use a person during the on-the-job portion of training to perform security functions provided that the person is closely supervised and does not make independent judgments as to whether persons or property may enter a sterile area or aircraft without further inspection.

(c) No certificate holder shall use a person to perform a screening function after that person has failed an operational test related to that function until that person has successfully completed the remedial training specified in the certificate holder's security program.

(d) Each certificate holder shall ensure that a Ground Security Coordinator conducts and documents an annual evaluation of each person assigned screening duties and may continue that person's employment in a screening capacity only upon the determination by that Ground Security Coordinator that the person:

(1) Has not suffered a significant diminution of any physical ability required to perform a screening function since the last evaluation of those abilities.

(2) Has a satisfactory record of performance and attention to duty.

(3) Demonstrates the current knowledge and skills necessary to courteously, vigilantly, and effectively perform screening functions.

(e) Paragraphs (a) through (d) of this section do not apply to those screening functions conducted outside the United States over which the certificate holder does not have operational control.

(f) At locations outside the United States where the certificate holder has operational control over a screening function, the certificate holder may use screeners who do not meet the requirements of paragraph (a)(3) of this section, provided that at least one representative of the certificate holder who has the ability to functionally read and speak English is present while the certificate holder's passengers are undergoing security processing.

LIST OF REFERENCES

1. White House Commission on Aviation Safety and Security (Gore Commission), *Final Report to The President,* 12 February 1997, available from www.aviationcommission.gov, accessed 2 January 1998.

2. President's Commission on Aviation Security and Terrorism (Bush Commission), *Report to the President*, U.S. Government Printing Office (GPO), 15 May 1990.

3. Department of Transportation (DOT) Office of Inspector General (DOTIG), *Audit of Airport Security*, Federal Aviation Administration (FAA), Report No. RP-FA-3-105, DOTIG Public Affairs Office Press, 20 September 1993.

4. DOTIG, *Efforts to Improve Civil Aviation,* FAA, Report No. R9-FA-6-014, DOTIG Public Affairs Office, 3 July 1996.

5. Ott, James, *A Broader Plan, Not a Silver Bullet*, Aviation Week and Space Technology (AW&ST), McGraw–Hill Companies, 7 October 1996: 32-34.

6. DOT, FAA Office of Civil Aviation Security (ACS). *Criminal Acts Against Civil Aviation: 1996*, FAA ACS, April 1997.

7. General Accounting Office (GAO), Report to Congressional Committees, *Aviation Security: Additional Actions Needed to Meet Domestic and International Changes*, Report No. GAO/RCED-94-38, U.S. GPO, 27 January 1994.

8. U.S. Department of State (DOS), *Patterns of Global Terrorism:1995*, U.S. DOS Office of the Coordinator for Counterterrorism, April 1996.

9. Higgens, Larry and Massola, Bob, SFO Police Department Detectives, interview by Ed Miller and Mark Dover, 9 January 1998.

10. Green, Larry, LT, LAX Special Projects Division/Security, interview by Ed Miller, 29 December 1997.

11. Yuen, Calvin, Manager, FAA ACS Western–Pacific Region, interview by Ed Miller and Mark Dover, 9 January 1998.

12. DOT, *FAR 107 Notice of Proposed Rule Making*, FAA ACS (ACP–100), U.S. GPO, 1 August 1997.

13. Montgomery, Melinda, Airport Operations Supervisor, San Jose International Airport, interview by Ed Miller and Mark Dover, 12 December 1997.

14. Wilkinson, Paul, *Designing An Effective International Security System*, Terrorism And Political Violence: Special Issue on Technology and Terrorism, Frank Cass, London, Vol. 5, No. 2, Summer 1993.

15. Wells, Alexander T., *Airport Planning and Management,* 3rd Edition, McGraw–Hill Companies, 1996.

16. GAO, Report to Congressional Committees, *Aviation Security: The FAA Can Help Help Ensure That Airports' Access Control Systems Are Cost Effective*, Report No. GAO/RCED -94-142, U.S. GPO, 1 March 1995.

17. Lane, Earl, *Dream Machine*, available from www.newsday.com, accessed 1
December
1997.

18. Schwartz, Ken, *Vendors Corner: Electronic Access*, available from www.nyarm.com, accessed 18 January 1998.

19. Bart, Krys T., A.A.E., Assistant Director of Aviation, San Jose International Airport, interview by Ed Miller and Mark Dover, 12 December 1997.

20. North America, Airports Council International, *Airports: The Facts*, available from www.mergeglobal.com, accessed January 1998.

21. Technological Solutions To Improve Aviation Security: Hearing Before The Committee on Science, U.S. House Of Representatives, 104th Congress, 2nd Session, U.S. GPO, 19 September, 1996.

22. Eisenburg, Carol, *A Tattered Security Blanket*, available from www.newsday.com, accessed 1 December 1997.

23. St. John, Peter, *Air Piracy, Air Security, and International Terrorism: Winning the War against Hijackers*, New York, Quorum Books, 1991.

24. Yan, Ellen, *Maginot Line for U.S. Aviation*, available from www.newsday.com, accessed 1 December 1997.

25. Staten, Clark, *Airport Safety and Security: Minimal Acceptable Standards*, available from www.emergency.com, accessed 1 December 1997.

26. Clark, John, *Illegals Access Airports and Employers given Slap on Wrist*, available from www.instanet.com, accessed 4 January 1998.

27. Nelson, Erik, *Security Supervisor at LAX Arrested: 21 October 1997*, Los Angeles News Channel 2000, available from www.kcbs2.com, accessed 4 January 1998.

28. *Computer Attendance Systems*, available from www.amertime.com, accessed 18 January 1998.

29. Madline, George, *Floyd Total Security*, available from www.floydtotalsecurity.com, accessed 18 January 1998.

INITIAL DISTRIBUTION LIST

1. Defense Technical Information Center 2
   8725 John J. Kingman Road, Suite 0944
   Fort Belvoir, VA 22060-6218

2. Dudley Knox Library 2
   Naval Postgraduate School
   411 Dyer Road
   Monterey, CA 93943-5101

3. Defense Logistics Studies Information Exchange 1
   U.S. Army Logistics Management College
   Fort Lee, VA 23801-6043

4. Commander United States Transportation Command (USTRANSCOM) 1
   (Code TCJ5–SE)
   508 Scott Drive
   Scott AFB, IL 62225-5357

5. Chief of Force Protection USTRANSCOM/TCFP 1
   Attn: Colonel James Van Ness
   508 Scott Drive
   Scott AFB, Il, 62225-5357

6. USTRANSCOM/TCRC 1
   Command Historian
   508 Scott Drive
   Scott AFB, IL 62225-5357

7. Commander 1
   Attn: NOO
   Military Sealift Command
   Washington Navy Yard, Building 210
   901 M-Street, SE
   Washington, DC 20398-5540

8. Federal Aviation Administration–Western Pacific Region 1
   Civil Aviation Security Field Office
   Attn: Mr. Calvin Yuen
   831 Mitten Road, Suite 102
   Burlingame, CA 94010

9. Donald R. Eaton RADM (Ret), (Code SM/Et) 1
Naval Postgraduate School
Monterey, CA 93943-5103

10. Prof. David G. Brown (Code SM/Bz) 1
Naval Postgraduate School
Monterey, CA 93943-5103

11. LCDR Edward G. Miller, USN 1
15559 Blues Creek Road
Marysville, OH 43040

12. LT Mark W. Dover, USN 1
134 Brownell Circle
Monterey, CA 93940