

Security Planning For General Aviation Airports



DISCLAIMER

This manual was produced by the Florida Airports Council to assist Florida's public general aviation airports in considering security-related issues and as an aid in preparing their airport's security plan.

This is an independent product of the Florida Airports Council and, as such, is not a product of, or officially endorsed by the Florida Department of Transportation, Florida Department of Law Enforcement, the Florida Legislature, the Department of Homeland Security, or any other state or federal agency.



August 13, 2004

Dear Florida Airport Manager:

As you are well aware, aviation represents a significant part of the state's economy. With 112 general aviation airports, 19 commercial service airports and a large number of military air bases, the economic impact from Florida's airports is enormous. We have the privilege of being the stewards of our state's airport system. Along with that stewardship comes the responsibility of keeping our airports, and those who use them, safe and secure.

The Florida Airports Council entered into a contract with the Florida Department of Transportation to develop a model security plan for general aviation airports which is contained in this three-ring binder. The information provided herein, regardless of your airport's size, type of customers you serve or operations conducted, should be beneficial in developing your airport's personalized security plan.

This manual is divided into four chapters; I. – *Introduction and Background*; II. – *Why Prepare an Airport Security Plan*; III. – *Examples of Airport Security Sections and Issues to be Considered*; and IV. – *The Model Plan*. The Model Plan is a template that can be used to create your airport's security plan. We have provided additional useful information in the Appendix section of the manual, including TSA's entire "*Security Guidelines for General Aviation Airports*".

Please remember, security is everyone's job. Basic security improvements are inexpensive. If you do not have a security plan in place, please take the needed time to develop at least a rudimentary plan. The goal of the Florida Airports Council is for each publicly-owned and operated airport in Florida to have a viable Airport Security Plan.

If you should have any questions or need additional assistance preparing your airport's security plan, please contact me and we will have a member of the General Aviation Committee assist you.

Please join us in assuring that Florida's airports are the safest in the nation. Due to the state's reliance on its airports to fuel its economy, we have an obligation to the citizens of Florida that no terrorist ever use one of our airports for their nefarious purposes.

Information provided in this report will be provided on FAC's webpage that may be downloaded for your use. If you are not a member of FAC or would rather have a disk to use in creating or modifying your airport's security plan, please contact the Florida Airports Council at (850) 224-2964 and we will send you one.

Sincerely,



William R. Johnson, AAE
Executive Director

Preface

This document was developed by the Florida Airports Council with a grant from the Florida Department of Transportation. We would like to acknowledge the efforts and assistance provided by the Transportation Security Administration (TSA) and members of FAC's General Aviation Committee and Technical Advisory Committee.

On behalf of the airport industry in Florida, we would like to thank all the members of FAC's General Aviation Committee; specifically, Gary Duncan, of the Lee County Port Authority, Chairman of the General Aviation Committee; Jason Milewski, of the Sebastian Municipal Airport; Rob Pruitt, of the Ocala International Airport; and Peter Modys, of the Lee County Port Authority and President of the Florida Airports Council for 2004.

We would also like to thank Bill Ashbaker, P.E., Aviation Office Manager of the Florida Department of Transportation, and Steven Calabro, of the Transportation Security Administration, for their guidance and support on this project.

TABLE OF CONTENTS

	<u>Page</u>
Disclaimer	i
Letter of Transmittal	ii
Preface	iii
Table of Contents	iv
Chapter	
I. Introduction (Tab 1)	1
Background	1
Study Advisory Committee and Technical Committee	1
Survey of Airports/Benchmarks	1
TSA Guidelines	1
Key Issues	3
GA Airport Vulnerability	3
Airport Characteristics	3
Florida Airports Council Review and Recommendations	4
Tier A	5
Tier B	6
Tier C	7
Tier D	8
Tier E	9
Recommendations to Individual Airports	9
Recommendations to FDOT	9
II. Why Prepare an Airport Security Plan (Tab 2)	11
Airport Security Measures	11
Monitoring Airport Property and Users	11
Controlling Movement on the Airport	12
Preventing Unauthorized Access to the Airport Operating Area (AOA)	12
Securing Unattended Aircraft	12
Reporting Unusual or Suspicious Activity	12
Airport Security Planning	12
The Airport Security Committee	13
Communications	13
What Should Be Considered in an Airport Security Plan	13
The Homeland Security Advisory System	14
Low (Green)	15
Guarded (Blue)	15
Elevated (Yellow)	15
High (Orange)	15
Severe (Red)	16
Appropriate Response to Increasing Levels of Risk	16

Protection of Airport Facilities	16
Hangars	16
Locks and Keys	16
Perimeter Control	17
Fences	17
Clear Areas	18
Access Points	18
Lighting	18
Signs	18
Identification System	19
Airport Planning	19
Surveillance	20
Airport Community Watch Program	20
Reporting Procedures	21
Law Enforcement Officer Support	21
Closed Circuit Television (CCTV)	21
Intrusion Detection Systems	22
Security Procedures and Communications	22
Security Procedures	22
Certain Information Exempt From Disclosure	22
Threat Level Increases	22
Threat Communication System	23
Airport Tenant Facilities	24
Aircraft and Vehicle Fueling Facilities	24
III. Examples of Airport Security Sections and Issues To Be Considered (Tab 3)	25
Attachment 1: Airport Watch Program	26
Attachment 2: Measures To Be Implemented Based On Threat Advisory Level	27
Attachment 3: Rules and Regulations Needed To Support	
General Aviation Security	30
Attachment 4: Airport Security Responsibilities	35
Attachment 5: Airport Lessee/Tenant/Employee Security Responsibilities	40
IV. Model Plan (Tab 4)	47
Cover Page	48
Table of Contents	49
Section I: Disclosure Statement/Security Responsibilities	50
Section II: General Information	51
Section III: Definitions and Terms	53
Section IV: Administration	58
Section V: Aircraft Movement Area/Security Control	59
Section VI: Airport Security Procedures	60
Section VII: Airport Emergency Grid Map	61
Section VIII: Identification of Airport Personnel	62
Section IX: Identification of Vehicles	63
Section X: Law Enforcement	64
Section XI: Special Events	65
Section XII: Increased Security Threats	66

Section XIII: Aviation Security Contingency Plans	67
Section XIV: Model Forms	68

Appendix

- A TSA Guidelines for General Aviation Airport Security (Tab 5)
- B Advisory Committee and Technical (Task Force) Committee Members (Tab 6)
- C FAC Phase One Report (Tab 7)
- D Report of the Aviation Security Advisory Committee Working Group (Tab 8)
- E AOPA's Airport Watch Program (Tab 9)

✦ ✦ ✦

CHAPTER I

INTRODUCTION

Background

Subsequent to the terrorist attacks of 2001, and the federal government's focus on the perceived higher risk commercial service airports, the Florida Airports Council (FAC) asked the Florida Legislature for funding to develop a model security plan for general aviation (GA) airports in Florida. The Florida Legislature approved this request and directed the Florida Department of Transportation (FDOT) to contract with FAC for this project. The Florida Airports Council, a Florida Not-For-Profit Corporation, represents all commercial service airports in Florida and a majority of the State's general aviation airports. FAC was formed in 1969 for the express purpose of improving and enhancing Florida's system of airports. After the terrorist attacks, the Board of Directors and membership of the Council felt that improved airport security, even at general aviation airports, was of critical importance to the recovery of the State's economy.

Due to the relationship between Florida's airports and the state's economic development and tourism economies, the Legislature felt the public needed to be assured the state's airports were as secure as possible. Florida's airports are as diverse as any state – from small, privately-owned grass fields to some of the nation's largest, heavy-use airports. The Airport Security Plan for General Aviation Airports, provided herein, is considered a model to be customized by each individual airport to suit their specific needs.

Study Advisory Committee and Technical Committee

An Advisory Committee was formed that consisted of commercial service and general aviation airports, as well as representatives from FDOT, the Florida Department of Law Enforcement (FDLE), and the Transportation Security Administration (TSA). In addition, a Technical Committee was formed that consisted of members of FAC's General Aviation Committee.

Survey of Airports/Benchmarks

All public airports in Florida were surveyed by FAC, with specific requests regarding self-assessments from each airport as to their strengths and weaknesses related to airport security. They were also asked about what security systems and/or programs they intended to undertake. Other states' aviation offices were contacted to ascertain what security initiatives their states had undertaken and benchmark airport programs were examined.

TSA Guidelines

Finally, in May of 2004, the Transportation Security Administration published "Security Guidelines for General Aviation Airports". This document was developed by TSA, in

cooperation with the General Aviation Community. It was intended to provide GA airport owners, operators, and users with guidelines and recommendations that address aviation security concepts, technology, and enhancements.

The recommendations contained in TSA's guidelines were developed in close coordination with a working group comprised of individuals representing the entire spectrum of the GA industry. TSA states that the document should be considered a 'living document' which will be updated and modified as new security enhancements are developed and as input from the industry is received.

TSA states that the purpose of the "*Security Guidelines for General Aviation Airports*" is to provide owners, operators, sponsors, and other entities charged with oversight of GA airports a set of federally endorsed security enhancements and a method for determining when and where these enhancements may be appropriate. The document does not contain regulatory language nor is it intended to suggest that any recommendations or guidelines should be considered a mandatory requirement.

The document offers a list of options, ideas, and suggestions for the airport operator, sponsor, tenant and/or user to choose from when considering security enhancements for GA facilities. This guidance will provide consistency across the nation.

The "*Airport Characteristics Measurement Tool*", included in TSA's guidelines, is a self-administered method by which an airport operator can assess an airport's security characteristics and decide which security enhancements would be most appropriate in that particular environment. TSA outlines seven functional areas of GA airport security, which are:

- Personnel
- Aircraft
- Airports/Facilities
- Surveillance
- Security Plans and Communications
- Specialty Operations

A copy of TSA's guidelines is provided as Appendix "A" to this report. TSA states it is 'Version 1.0' and they expect to be updating the guidelines from time to time, based on input from the GA community. In addition, the Florida Airports Council will maintain a secure web site at www.floridaairports.org to provide the latest updates from the federal government on general aviation security. Each airport should monitor this website on a regular basis for the latest security information from the federal and state government.

Key Issues

→ GA Airport Vulnerability

TSA states that it has not taken a position that GA airports and aircraft are a threat, in and of themselves. However as vulnerabilities within other areas of aviation have been reduced, GA may be perceived as a more attractive target and consequently more vulnerable to misuse by terrorists. TSA believes that its security guidelines will help airport managers determine which security measures they should take at their particular facility to reduce vulnerabilities and encourage the adoption of consistent and appropriate security measures across the nation. TSA also believes that federal endorsement of their security guidelines will discourage a hodgepodge of state and local guidelines.

TSA states that “one size – fits all” security will not fit the entire spectrum of GA airports. Instead, TSA focuses on managing the risk associated with GA facilities recognizing the characteristics that define each facility. They state that the decision to implement security measures must include consideration of economic feasibility and reasonableness.

→ Airport Characteristics

TSA created a measurement tool that airport managers can utilize to identify what makes each individual airport unique. *“The Airport Characteristics Measurement Tool”* identifies several categories that must be considered when assessing potential security vulnerabilities and remedies. They are:

- Airport Location (proximity to mass population areas)
- Number of Based Aircraft (the higher the number of based aircraft, the less likely management can identify suspicious activities)
- Runway Length (airports with longer, paved runways are able to accommodate larger aircraft and should consequently be more security conscious)
- Operations (risk is increased with the higher number, and more varied types, of operations)

TSA assigned point values in each category and suggested security enhancements based on their point system. They recommended four tiers of airports nationwide, suggesting the nation’s lowest risk airports provide, at least, the following:

- Signage
- Documented Security Procedures
- Positive Passenger/Cargo/Baggage Identification
- All Aircraft Secured
- Community Watch Program
- Written Contact List

The next tier, with a slightly higher risk factor, should also consider adding:

- Law Enforcement Officer (LEO) Support
- An Airport Security Committee
- Transient Pilot Sign-In/Sign-Out Procedures

The third tier should consider adding:

- Access Controls
- Lighting System
- Personal Identification System
- Vehicle Identification System
- Challenge Procedures

The highest risk category should consider adding:

- Fencing
- Hangars (as security tools)
- Closed-Circuit Television
- Intrusion Detection System

They also recognized that there are mitigating characteristics that positively affect the scoring, such as;

- Operating Air Traffic Control Tower
- 24/7 Airport Staffing
- Law Enforcement Personnel on Airport Property
- All Based Aircraft less than 1,500 lbs
- All Grass Runways
- Restricted Access to Airport
- Required Identification Badges
- Documented Security Procedures

Florida Airports Council Review and Recommendations

In preparing this Model Plan for Florida's airports, FAC's Technical Committee reviewed TSA's recommendations and concurred that each airport is unique and a "one size – fits all" solution is not appropriate (especially in Florida) and that FDOT's grant program makes the state's general aviation airports more capable of providing a much higher level of security than other states.

The committee felt strongly that each general aviation airport in the state needed an Airport Security Plan. It also felt the plan did not have to be complex and that a small airport could have a plan that was simple, inexpensive, and yet a valuable tool to communicate the importance of airport security to local governmental leaders, airport tenants and users, law enforcement agencies, and the general public.

The committee indicated that as a minimum each airport manager should:

- Get to know each tenant, their employees and owners/operators of based aircraft.
- Get to know what belongs at the airport and what does not
- Form an airport watch group, and an airport security committee with regular meetings – at least quarterly
- Encourage all tenants to lock their hangars, their aircraft, and all doors and gates
- Perform an Airport Security Assessment to determine vulnerabilities
- Write a Security Plan (using this Model Manual, TSA’s Guidelines, or create your own)

TSA’s recommendations and the following chapters of this manual provide examples of security measures for Florida’s GA airports. Chapter IV of this manual is a model that each airport can use in developing its own plan.

The recommendations herein are provided specifically for airport and facility managers but additional information regarding tenants, airport users, and specialty operators is provided, as well.

Florida’s landmark state grant program has resulted in a much higher state standard for general aviation security compared to the national average. For this reason, and because Florida is a highly urbanized state, the Technical Committee recommended a higher standard for our state.

The Technical Committee also recommended Florida consider adopting a non-mandatory tiered system for airport security, with each airport selecting the appropriate tier for that facility based on its risk assessment. Although this tiered system would not be compulsory and would not affect grant funding in any manner, the Technical Committee recommended that within a year FDOT formally acknowledge which airports had written security plans. The ultimate goal would be to have each public airport operating at least at the Tier “A” level within a year of the publication of FAC’s model manual.

The tiers recommended by the Technical Committee varied from TSA’s recommendations slightly because of Florida’s airport’s ability to secure 100% FDOT funding for security-related capitol projects.

Tier A

- **Written Security Plan**

The first criterion is the development of a written security plan, utilizing information from FAC’s Model Plan, TSA’s Guidelines for GA Security, or others.

- **Signs**

“No Trespassing” and/or “Restricted Area” type signs should be placed in visible areas to help prevent unauthorized access to the AOA. Any and all restricted areas need to be clearly identified.

- **Lighting**

Aircraft/vehicle parking areas, walkways, and buildings should be well lit so that activities in these areas can be seen from a distance at night. In addition, any additional areas where someone could hide (such as dark corners, architectural enclaves, landscape hedges, etc.) should be identified and lit, if possible. If cameras are to be used, be sure to coordinate with the installer/manufacturer to obtain the most effective types of lighting.

- **“Best Practices Program” Awareness Brochures/Training**

Increasing awareness is likely the most effective measure in improving security. Airport security should always be a topic of discussion at periodic tenant meetings. Flyers and signs containing contact information for suspicious activities should be placed in all high traffic areas. AOPA’s *Airport Watch* Program is an excellent method of increasing awareness and educating airport users. Airport managers are encouraged to employ this or develop their own program. Information on AOPA’s *Airport Watch* is provided in the Appendix section of this manual.

- **Local Law Enforcement Patrols**

At this level, airport managers are simply recommended to meet with local law enforcement personnel with jurisdiction over the airport, provide them rudimentary training on airport issues, policies and procedures, and seek their cooperation in routine airport patrols. Exchange of emergency contact information is imperative in the event of an airport emergency.

Tier B

This should include all chosen components from Tier A as well as:

- **Entry Barriers**

Fences, hedging, barricades, etc. should be installed in high traffic and/or other vulnerable areas to discourage unauthorized access to the AOA. Thorny plants and hedges make for useful, natural, and aesthetically pleasing barriers for personnel. Chained entryways aid in deterring vehicles from entering restricted areas. Ranch-style farm fencing and cattle gates are inexpensive and effective methods of accomplishing fencing needs.

- **Based Aircraft Inventory**

An inventory of all based aircraft should be kept on file in the airport manager's office. This should contain the registration number, make, model, registered owner's name, address, phone, emergency contact information, and operator's name and contact information (if different from owner). This will not only aid in keeping track of what is based at the airport, but also allow for immediate contact of aircraft owners in the event of an emergency (i.e. fire, theft, wind damage, etc.). As a component of this Security Plan, this inventory shall be exempt from public record laws.

- **Transient Aircraft Logs (FBO Participation)**

Tenants should keep a record of transient aircraft parking and/or fueling at the airport. This should contain the make, model, and registration number of the aircraft as well as the time and dates of arrival and departure. As a component of this Security Plan, this log shall be exempt from public record laws.

- **Airport/Tenant Employee List**

A complete listing of all airport employees, tenant employees should be prepared, and updated on a regular basis, with addresses and all necessary telephone numbers.

- **Local Law Enforcement Liaison**

A formal arrangement should be made with local law enforcement to make regular patrols of airport property. Records of such patrols should be kept on file in the airport manager's office. Numbers and intensity of patrols should correlate to National Threat Level as declared by the Department of Homeland Security. A formal liaison officer should be appointed as a direct contact between airport management and law enforcement (*Airport Security Liaison*) that is fully trained on airport rules, regulations, and procedures and would provide the necessary training for other LEO's patrolling the airport environment.

Tier C

This should include all chosen components from Tiers A and B; plus:

- **Standardized, Complete Perimeter Fencing**

The entire AOA should be fenced with no less than a six foot high, chain link fence with three strands of barbed wire on top, if feasible. Unmonitored access gates should be secured. All tenants should be held responsible for controlling access through their leased premises to the AOA.

- **Law Enforcement with Living Quarters at Airport**

The airport should make available suitable living quarters for an LEO to reside at the airport to provide quick response in the event of an airport emergency, similar to what is common practice at many public schools. Several airports in Florida have instituted this program and have reported a high level of success.

- **Restricted Area Personnel/Vehicle Identification Program**

All authorized personnel in the AOA or other restricted areas should wear airport-issued identification badges. All vehicles operating in the AOA shall display an authorized pass or badge. This aids local law enforcement in determining who is and who is not authorized to be in a restricted area. This also helps airport administration record contact information for those who require access to the AOA and/or other restricted areas. See Chapter IV (Model Forms) for “*Airport Identification Badge Application*” form. As a component of this Security Plan, this information shall be exempt from public record laws.

Tier D

This should include all chosen components from Tiers A - C; plus:

- **Video Surveillance**

Cameras should be installed to monitor aircraft and vehicle parking areas, AOA access points, and/or any other areas of vulnerability. If possible, digital recording media is recommended, as well as a monitoring station in the local law enforcement dispatch center. This will ensure that activities are viewed twenty-four hours per day and that police response is summarily executed. Be sure to investigate the need for any additional and/or special types of lighting, if applicable.

- **On-Site Law Enforcement/Security Personnel**

The airport should employ (either directly or by contract) law enforcement or certified security personnel to *exclusively* offer on-site airport security services. This can be for the previously discussed *Airport Security Liaison* or other officer.

- **Electronic Access Control to Restricted Areas**

Access to the AOA through unmonitored gates should be electronically controlled via keypads, proximity cards, and/or other methods. Records of such access should be kept on file in the airport manager’s office. As a component of this Security Plan, this information shall be exempt from public record laws

Tier E

This should include all chosen components from Tiers A - D above; plus:

- **24 hour Law Enforcement/Security Service**

The airport should employ (either directly or by contract) law enforcement or certified security personnel to exclusively offer on-site airport security services *twenty-four hours per day*.

- **Air Traffic Control Tower**

The airport should have an air traffic control tower, which has the added benefit of monitoring the AOA while in operation. It is recommended that the operating hours of the tower be extended as necessary for maximum coverage of the airport

- **Electronic Perimeter Protection**

Electronic perimeter protection should be installed along the entire fence line to detect a breach and/or intrusion attempt. It is recommended that this system be integrated with cameras to record alarm events

- **Landside Video Surveillance covering Access Roads**

All access roads leading to and from the airport should have cameras installed to monitor and record vehicles entering and leaving airport property

Recommendations to Individual Airports

In addition to the Security Tiers, the Technical Committee suggested that each airport consider the following:

- Conducting a 'vulnerability assessment' prior to completing its Security Manual and conducting a 'self-assessment' of its security programs every six months
- Contacting the airport's insurance provider to determine whether development of a security plan could decrease the airport's insurance premium(s)
- Security plans are exempt from public disclosure and these plans should be available only to those with demonstrated need-to-know.

Recommendations to Florida Department of Transportation

The Technical Committee also suggested that over the next 12 months, the Florida Department of Transportation consider the following issues:

- Increasing state and federal funding for general aviation airport projects

- Removing the 2007 expiration of the grant program that allows FDOT to fund one hundred percent (100%) of eligible security projects, making that a permanent funding program
- Increasing the penalties for trespassing and tampering with security devices at airports
- Increasing the number of air traffic control towers at GA airports as security enhancements
- Creating a state standard for ID/vehicle badging at GA airports
- Development of annual training programs for law enforcement officers and airport personnel on security-related issues
- Development of state-wide promotional materials for airport users, tenants, etc. on airport security issues.
- Development, with the Florida Airports Council, of a 'Peer Review' program, with volunteers to assess each airport's security plan every 2-3 years.

✈ ✈ ✈

CHAPTER II

WHY PREPARE AN AIRPORT SECURITY PLAN

Due to immense public and congressional concern and scrutiny, the Transportation Security Administration (TSA) has placed great emphasis on increasing security at commercial service airports, and considers general aviation airports of lower risk. Since there are relatively small congregations of people at GA airports, it is felt the main threat is not against the airport itself, but rather the unauthorized use of aircraft located at the facility for an illegal purpose.

TSA has stated that each airport should develop a plan to prevent:

- Theft or unauthorized use of an aircraft that could be used as a weapon
- Use of an airport as a site of departure by a terrorist
- An act of sabotage to aircraft against based and/or transient aircraft users and passengers
- An act of sabotage on an airport against airport tenants and/or facilities

AIRPORT SECURITY MEASURES

Regardless of the size or operational characteristics of a particular facility, it is strongly recommended that all public-use airports adopt reasonable security standards and procedures to (1) monitor airport property and users, (2) control the movement of persons and ground vehicles on airport property, (3) prevent unauthorized access to the AOA, (4) secure unattended aircraft, and (5) report unusual or suspicious activity.

The following suggestions are provided in an effort to help each airport manager and security committee consider the salient issues affecting their facility. The unique nature of each airport in Florida will undoubtedly result in Airport Security Plans of various complexities. Security issues to be considered are:

Monitoring Airport Property and Users

Airport owners should take reasonable measures to monitor and protect airport users, visitors, guests, and airport property including buildings, facilities, and equipment. Suggested measures include regular inspections of airport property and facilities (e.g. AOA, fence lines, fuel trucks, storage buildings, and NAVAIDS), requesting periodic inspection/patrol by local law enforcement, and, if warranted, employment of local law enforcement officers on a part-time basis. Airport managers should also install locks on airfield electrical vaults, fuel cabinets, tank fill hatches and pumps, and power shutoff switches.

Airport managers should consider implementing a Neighborhood Watch Program for their airport by organizing the voluntary participation of based pilots, airport tenants and

users to help monitor aircraft storage areas (e.g. apron and hangars) and to report unusual or suspicious activity to airport management.

Controlling Movement on the Airport

Airport managers should take reasonable measures to control the movement of persons, aircraft, and ground vehicles on airport property. Suggested measures include installation of security fencing to protect against inadvertent or unauthorized access to the AOA, closing vehicular and pedestrian gates leading into the AOA, locking or monitoring gates when not in use, and requiring leasehold tenants to develop their own security plans. Signage, lights, and markings are also an important part of controlling movement on the airport by providing clear direction to airport users. Installing airport user signs, aircraft guidance signs, airfield lights, and pavement markings (pursuant to applicable FAA standards) will facilitate safe and efficient movement on the airport, which enhances airfield security by providing better control of AOA activity.

Preventing Unauthorized Access to the Airport Operating Area (AOA)

Airport managers should take measures to discourage unnecessary pedestrian and vehicular access into, and movement within, the AOA. If conditions warrant and funding permits, fencing, gates, and access control devices should be installed where appropriate. Segregating aircraft and private ground vehicles increases airport safety and security.

Securing Unattended Aircraft

Airport owners should strongly encourage, or require, that all based aircraft owners take reasonable measures to prevent the theft and illegal operation of their aircraft. Possible options include installing an anti-theft device and/or a device to lock aircraft flight controls when not in use, other lockable devices to secure their aircraft to the ground, and locking the doors on aircraft storage hangars at all times when not in use. At a minimum, aircraft owners should be required to remove the keys to their aircraft and lock all doors when not in use.

Reporting Unusual or Suspicious Activity

All airports should provide instructions to airport users and the general public for reporting unusual or suspicious activity.

AIRPORT SECURITY PLANNING

Proper and thorough planning is the key to good airport security. All public-use airports, regardless of size, should develop their own Airport Security Plan based on suggestions from this document, and from state and federal officials, tailored to each specific airport and operational conditions. However, creating and implementing such a plan is very much a team effort requiring input, coordination, and cooperation with various parties.

The Airport Security Committee (ASC)

To improve coordination, gain different perspective, and increase plan acceptance, airport owners should create an Airport Security Committee. The ASC should consist of representatives from airport management, airport tenants, airport users, local public safety emergency management, and other appropriate parties. The primary purpose of the ASC is to advise the airport owner on issues to consider in improving airport security. Good communication and cooperation between all parties is essential for balancing the desire for public access and utility with the need for public safety and security.

Communications

Communication is critical to an effective Airport Security Plan. Airport managers should consider the following communication processes and procedures:

- Contacting local law enforcement agencies and verifying the procedures used to report suspicious activity
- Developing a process to facilitate determining whom to call (a contact plan)
- Circulating these reporting procedures to all tenants and others who have a regular presence on the airport
- Directing aircraft owners and pilots to report suspicious activity to police and airport management, and/or other authorities
- Establishing a transient aircraft log
- Encouraging all tenants and based aircraft owners to comply with the airport's reporting procedures, as well as supplying a copy of the procedures and contact numbers, as appropriate
- Developing communication procedures to disseminate security information to airport tenants, the flying public, and local public safety agencies, as appropriate
- Conducting regular meetings with airport tenants and based aircraft owners to discuss the security issues and challenges. This involvement will help to get their 'buy-in' should any procedures or policies need to be added or revised
- Having a qualified, single point of contact for disseminating security information on a limited 'need to know' basis

Communication and reporting systems should be in place and understood by all involved in the event an unusual occurrence is observed.

What Should Be Considered in an Airport Security Plan

Airport managers should consider the following issues, as a minimum:

- Tailoring the Airport Security Plan for that specific airport
- Creating and implementing an ASP will take a team effort, requiring coordination and cooperation of local, state, and federal authorities, as well as private end users. Therefore, airport management should assemble an Airport Security Committee (ASC) to advise/assist management in developing its ASP.

- Listing and clearly defining the different types of airport users and the hours of operation for each user. The list may include airlines, FBO'S, maintenance facilities, fueling operators, flight schools, based aircraft owners, flying clubs, transient operators, restaurants, etc. Aircraft owners can be considered as one group.
- Maintaining a list of airport users. Review it for accuracy, update as necessary, and incorporate the list into the ASP.
- Discussing the access requirements for each specific user, with particular emphasis on those that require access to the airside area. Access to the airside area by employees, visitors, guests, mail, and package delivery requirements should be discussed in detail.
- Discussing the security requirements and emergency response issues for each user
- Advising airport tenants to evaluate their operations from a security standpoint and institute policies and procedures appropriate to their specific business. This evaluation can be done by conducting a policy, procedure and physical security audit to determine security deficiencies.
- If applicable, the airport should recommend tenants develop their own security plan, complying with their Airport Security Plan, and meet, at minimum, federal guidelines. Tenant security plans should be incorporated into the Airport's Security Plan.
- Designating a qualified employee as a security coordinator to be responsible for maintaining, upgrading, and updating any security policies and procedures
- Developing and incorporating standard procedures to report all unusual and suspicious activities to local law enforcement or the appropriate agency
- Incorporating emergency response considerations
- Developing or updating access plans to the airside area
- Developing procedures to monitor who is using the airport (e.g. greet all arriving strangers, both air and landsides)
- Developing a process to close the airport and restrict access to runways if directed by the Transportation Security Administration or Federal Aviation Administration

Security-sensitive information should be disseminated only to those with an operational 'need to know'. Also, airport management should recognize that at general aviation airports, many of the tenants are retail establishments. As such, they must have a realistic way that their customers can access them in a simple manner, without compromising security

The Homeland Security Advisory System (HSAS)

The Homeland Security Advisory System has provided a comprehensive and effective means to disseminate information regarding the risk of terrorist attacks to federal, state, and local authorities and to the American public. As part of a series of initiatives to improve coordination and communication among all levels of government and the American public in the fight against terrorism, President Bush signed the Homeland Security Presidential Directive 3, creating the Homeland Security Advisory System (HSAS). The advisory system is the foundation for building a comprehensive and

effective communication structure for the dissemination of information regarding the risk of terrorist attacks to all levels of government. The HSAS establishes the following five Threat Conditions with associated suggested Protective Measures. HSAS levels are:

Low (Green) - *Low risk of terrorist attacks*

The following Protective Measures should be considered:

- Refining and exercising preplanned Protective Measures
- Ensuring personnel receive training on HSAS, departmental, or agency-specific Protective Measures
- Regularly assessing facilities for vulnerabilities and taking measures to reduce them

Guarded (Blue) - *General risk of terrorist attack*

In addition to the previously outlined Protective Measures, the following should be considered:

- Checking communications with designated emergency response or command locations
- Reviewing and updating emergency response procedures
- Providing the public with necessary information

Elevated (Yellow) - *Significant risk of terrorist attacks*

In addition to the previously outlined Protective Measures, the following should be considered:

- Increasing surveillance of critical locations
- Coordinating emergency plans with nearby jurisdictions
- Assessing further refinement of Protective Measures within the context of the current threat information
- Implementing, as appropriate, contingency and emergency response plans

High (Orange) - *High risk of terrorist attacks*

In addition to the previously outlined Protective Measures, the following should be considered:

- Coordinating necessary security efforts with armed forces or law enforcement agencies
- Taking additional precaution at public events
- Preparing to work at an alternate site or with a dispersed workforce
- Restricting access to essential personnel only

Severe (Red) - Severe risk of terrorist attacks

In addition to the previously outlined Protective Measures, the following should be considered:

- Assigning emergency response personnel and pre-positioning specially trained teams; monitoring, redirecting or constraining transportation systems
- Closing public and government facilities
- Increasing or redirecting personnel to address critical emergency needs

Appropriate Response to Increasing Levels of Risk

Each airport manager and/or Airport Security Team should consider that airport's appropriate response to increasing levels of risk, and should include that response in the airport's Airport Security Plan. Although GA airports are considered lower risk than commercial airports by the federal government, due to Florida's size, urban nature, and importance of aviation to the state's economy, security is of prime importance to the state's leaders and citizenry.

PROTECTION OF AIRPORT FACILITIES

Protection of airport facilities is among the most important duties of the airport owner and/or manager. The following suggestions should be considered when preparing an Airport Security Plan:

Hangars

Storage in hangars is one of the most effective methods of securing general aviation aircraft. Every attempt should be made to utilize hangars when available and ensure that all hangar/personnel doors are secured when unattended.

Hangars should be properly marked and numbered for ease of emergency response. These areas are also a good place to install security and informational signs. Hangar locks that have keys that are easily obtained or duplicated should be avoided. Hangar locks should be re-keyed with every new tenant. Proper lighting around hangar areas should be installed. As an additional security measure, alarm and intrusion detection systems could also aid in the security of hangars.

Locks and Keys

Locks are an integral part of airport and aircraft security. In addition to their physiological deterrence, their physical strength and resistance to all but the most determined thief provides security in itself. It is important that the manager of a facility knows each employee who has access to each lock.

Key control is as important as the use of locks and includes control of keys, key codes, key cutting and combination equipment, and key issuance and retrieval. Rigid controls should be established to ensure that:

- If systems requiring key cutting codes and equipment are used, measures are taken to protect them against loss or misuse
- Key issuance authority is limited to as few personnel as possible to minimize improper distribution
- Keys are issued to personnel on the basis of operational needs and not as a convenience
- Keys are retrieved when personnel leave the airport by transfer, dismissal, resignation, or lease expiration
- Lost keys are reported promptly to the appropriate airport personnel
- Un-issued locks and keys are properly safeguarded
- Keys are stamped or engraved with "Do Not Duplicate"
- The key issuance system is periodically audited to ensure accountability for all keys

Perimeter Control

To delineate and adequately protect secure areas from unauthorized access it is important to consider boundary measures such as fencing, walls, or other physical barriers, electronic boundaries, and/or natural barriers. Physical barriers can be used to deter and delay the access of unauthorized persons onto sensitive areas of airports. Such structures are usually permanent and are designed to be a visual and psychological deterrent as well as a physical barrier. They also serve to meet safety requirements in many cases. Where possible, fencing or other physical barriers should be aligned with security area boundaries. The effective of this is dependent on the quality of the airport's overall security plan.

Fences

Some basic fencing features that enhance security include:

- **Height** – the higher the barrier, the more difficult and time consuming to breach
- **Barbed wire** – adding barbed wire at the top of the fence increases the level of difficulty and time to breach
- **Eliminating handholds** – omitting a rail at the top of the fence makes the fence more difficult to climb
- **Burying the bottom of the fencing** – eliminates the possibility of forcing the mesh up so that individuals can crawl under
- **Sensor System** – addition of an intrusion/alert system adds another level of security to the perimeter
- **Lighting** – increases visibility and raises the level of psychological deterrent
- **Signage** – installed along the fence line, signs are important to indicate private secured areas and the presence of security patrols, alarms, or monitoring systems

Clear Areas

Security effectiveness of perimeter fencing is materially improved by the provision of clear areas on both sides of the fence, particularly in the vicinity of the terminal and any other critical facilities. Suggested clear distances range from 10 to 30 feet, within which there should be no climbable objects, trees, or utility poles abutting the fence line, nor areas for stackable crates, pallets, storage containers, or other materials. Parking of vehicles along the fence should be minimized. Landscaping should be minimized or eliminated to reduce potential hidden locations for persons, objects, fence damage, and vandalism.

Access Points

Access point type and design may be the determining factor in the effectiveness of the security boundary. The number of access points should be minimized and their use and conditions regularly monitored.

Gates should be constructed and installed to the same or greater standard of security as any adjacent fencing in order to maintain the integrity of the area. All gates should have self-closures and be equipped so that they can be secured should enhanced security conditions require it. All gates should be sufficiently lighted.

For vehicle access, limiting the size of the opening increases security, reduces the possibility of one vehicle passing another and shortens the open/close cycle time.

Lighting

A careful analysis of security lighting requirements should be based on the need for good visibility and the following criteria: employee recognition and badge identification, vehicle access, detection of intruders, and deterrent to illegal entry.

Outdoor area lighting can help improve the security of aircraft parking and hangar areas, fuel storage areas, airport access points, and other appropriate areas. Lighting units for perimeter fences should be located a sufficient distance within the protected area and above the fence so that the light pattern on the ground will include an area on both the inside and the outside of the fence.

Signs

The use of signs provides a deterrent by warning of facility boundaries as well notifying of the consequences for violation. While signs for security purposes should be designed to draw attention, it also should be coordinated with other airport signs for style and consistency when possible.

Wording may include – but is not limited to – warnings against trespassing, unauthorized use of aircraft and tampering with aircraft, and reporting suspicious activity. Signage should include phone numbers of the nearest responding law enforcement agency, 911 (*for emergencies*), or TSA’s 1-866-GA-SECURE, whichever is appropriate.

For more information, refer to Advisory Circular (AC) No: 150/5360-12D, Airport Signing and Graphics. International airports should consult the International Civil Aviation Organization (ICAO) Document 9430-C/1080, International Signs to Provide Guidelines to Persons at Airports.

Identification System

Airports may want to consider implementing a method of identifying airport employees or authorized tenant access to various areas of the airport. These systems can range from a simple laminated identification card that includes a photograph of an individual to a sophisticated swipe card with various biometric data. Procedures should be developed that include ensuring control and accountability of the media. Elements that should be considered as part of an identification system should include:

- A full-face image
- The individual’s full name
- Airport name
- Employer
- A unique identification number
- The scope of the individual access and movement privileges
- A clear expiration date

In addition, a vehicle identification system may be developed. Such a system can assist airport personnel and law enforcement in identifying authorized vehicles. Vehicle identification can be through the use of decals, stickers, or hang tags. More suggestions for establishing an identification system can be found in AC-107-1, “Aviation Security – Airports”.

Airport Planning

Planning for security should be an integral part of any project undertaken at an airport. The most efficient and cost effective method of instituting security measures into any facility or operation is through advance planning and continuous monitoring throughout the project. Selecting, constructing, or modifying a facility without considering the security implications can result in costly modifications and delays. Airport operators should consider addressing future security needs such as access controls and lighting enhancements when planning new hangars or terminal buildings. Security concerns should be included and addressed in airport facility and land leases, airport rules and regulations, and the minimum standards document. In addition, airport construction projects can affect airfield security. Construction personnel and vehicle access during projects should be considered.

Surveillance

The vigilance of airport users is one of the most prevalent methods of enhancing security at GA airports. Teaching an airport's users and tenants what to look for with regard to unauthorized and potentially illegal activities is essential to effectively utilizing this resource. Airport managers can either use an existing airport watch program (such as AOPA's Airport Watch) or establish their own airport specific plan.

Airport Community Watch Program

An Airport Community Watch program, as previously discussed, should include elements similar to those listed below. Additional measures that are specific to each airport should be added as appropriate, including:

- Coordinating the program with all appropriate stakeholders including airport officials, pilots, businesses and/or other airport users
- Holding periodic meetings with the airport community
- Developing and circulating reporting procedures to all who have a regular presence on the airport
- Encouraging proactive participation in aircraft and facility security and heightened awareness measures. This should include encouraging airport and line staff to 'query' unknowns on ramps, near aircraft, etc
- Posting signs promoting the program and warning that the airport is watched. Include appropriate emergency phone numbers on the sign
- Installing a bulletin board for posting security information and meeting notices
- Providing training to all involved for recognizing suspicious activity and appropriate response tactics. This could include the use of a video or other media for training. The following are some recommended training topics:
 - Aircraft with unusual or unauthorized modifications
 - Persons loitering for extended periods in the vicinity of parked aircraft, in pilot lounges, or other areas deemed inappropriate
 - Pilots who appear to be under the control of another person
 - Persons wishing to rent aircraft without presenting proper credentials or identification
 - Persons who present apparently valid credentials but who do not display a corresponding level of aviation knowledge
 - Any pilot who makes threats or statements inconsistent with normal uses of aircraft
 - Events or circumstances that do not fit the pattern of lawful, normal activity at an airport
- Utilizing local law enforcement for airport security community education.
- Encouraging tenants to make their staff aware of the airport watch programs.

Reporting Procedures

It is essential that every airport employee, tenant, and user is familiar with reporting unusual or suspicious circumstances on airport property. There are three basic ways that persons can report suspect activities.

- Contact airport management
- Utilize the GA-SECURE hotline (the National Response Center). 1-866-GA-SECURE operates 24 hours per day, 7 days per week.
- Contact local law enforcement using a local phone number. In instances where the situation could potentially turn dangerous all pilots are strongly encouraged to dial 911. After contacting 911 or airport management, TSA also recommends that callers contact the GA Hotline to ensure that information surrounding the incident reaches the National Response Center.

Law Enforcement Officer Support

It is imperative that airport operators establish and maintain a liaison with appropriate local, state, and federal law enforcement agencies. These organizations can better serve the airport operator when they are familiar with airport operating procedures, facilities, and normal activities. Procedures may be developed to have local LEOs regularly or randomly patrol ramps and aircraft hangar areas, with increased patrols during periods of heightened security.

Airport operators should communicate and educate local law enforcement agencies on operational and security procedures at the airport. This may include:

- Recognizing proper airport credentials (e.g. airport ID badges, airmen certificates, etc.)
- Recognizing those airport users authorized to drive on the ramp
- Notifying LEOs as to how they can obtain airport access (e.g. who has gate keys, access codes)
- Educating LEOs on airport speed limits, aircraft right-of-way procedures, and other 'normal' operations
- Issuing airport maps with a detailed facility index
- Recognizing 'normal' airport operations

Closed Circuit Television (CCTV)

In conjunction with a perimeter fence, CCTV may help deter security breaches at airports. and may provide an improved response when breaches do occur. CCTV video recorders may provide a visual record that can be used to document activities that become the subject of investigations. The inherent weakness of this system is that it must be monitored to be effective.

Intrusion Detection Systems

IDS are becoming more and more popular as a method for providing GA airport security. They can replace the need for physical security personnel to patrol an entire facility or perimeter. If an intrusion or some other specified event (e.g. fire or power outage) is detected, the system administrator notifies police, fire, and/or airport management.

SECURITY PROCEDURES AND COMMUNICATIONS

Security Procedures

TSA states that written security procedures are helpful for all the nation's general aviation airports. The Florida Airports Council's Technical Committee feels that, because of Florida's strategic location, reliance on tourism and economic development, each general aviation airport in Florida should have a written security plan. In fact, the committee has recommended that in the future FDOT require each publicly owned and operated airports to have written security plans.

A written plan provides managers with a traceable and auditable method of ensuring airport employees and tenants are aware of and understand security issues. Since these plans may contain sensitive information the airport operator should limit access to these plans. The State of Florida passed legislation that exempts airport security plans from public information. This may be found in Section 331.22, Florida Statutes., which states:

Certain information exempt from disclosure.

Airport security plans of an aviation authority created by act of the Legislature or of an aviation department of a county or municipality which operates an international airport are exempt from provisions of s. 119.07(1) and s. 24(a), Art. I of the State Constitution. In addition, photographs, maps, blueprints, drawings, and similar materials that depict critical airport operating facilities are exempt from the provisions of s. 119.07(1) and s. 24(a), Art. I of the State Constitution, to the extent that an aviation authority created by act of the Legislature or an aviation department of a county or municipality which operates an airport reasonably determines that such items contain information that is not generally known and that could jeopardize the security of the airport; however, information relating to real estate leases, layout plans, blueprints, or information relevant thereto, is not to be included in this exemption. The exemptions in this section are applicable only to records held by an aviation authority created by act of the Legislature or to records of a county or municipal aviation department that operates an airport.

Threat Level Increases

The Homeland Security Advisory System (HSAS), discussed previously, is a mechanism for the Department of Homeland Security to disseminate information regarding the risk of terrorist acts throughout the nation. It provides airport operators with information to

implement increased security measures during times of heightened alert and to reduce security procedures at lower threat levels.

Each Airport Security Plan should include reference to and be coordinated with appropriate local response plans. The protocol should emphasize such critical elements as awareness, prevention, preparation, response, and recovery.

During times of lower alert levels (Green, Blue, and Yellow) airport operators may wish to do the following:

- Develop preparedness plans, emergency contact lists, and training programs to ensure key elements of HSAS and preparedness plans are presented to all employees
- Review and update any previously developed preparedness plans, emergency contact lists, and training programs
- Communicate with appropriate local federal agency representatives (e.g. DHS, FBI, and TSA)
- Conduct surveillance of facility property, buildings, and aircraft
- Coordinate emergency plans as appropriate with nearby jurisdictions
- Hold security committee meetings to ensure timely dissemination of security/threat information

Appropriate actions for increased alert levels (Orange or Red) may include:

- All measures from lower level alerts (see above)
- Limiting facility access points
- Making regular surveillance patrols of facility property, buildings, and aircraft
- Increasing surveillance of critical locations
- Coordinating necessary security efforts with federal, state, and local law enforcement agencies or any National Guard or other appropriate organizations
- Preparing to execute contingency procedures, as appropriate
- Ensuring positive identification of pilots and tenants
- Assigning emergency response personnel, pre-positioning, and mobilize specially trained teams or resources
- Closing the facility, or parts of the facility

Threat Communication System

The development of a comprehensive contact list is vitally important and must be included in the Airport Security Plan. The list should be distributed to all appropriate individuals. The following phone numbers, *as a minimum*, should be included on the contact list (include after hour contact numbers where appropriate):

- Airport management
- Airport security contacts
- Local police or sheriff departments (List all responding LEO agencies)

- FDOT Aviation Office Director and district aviation personnel
- county/city emergency manager
- FDLE contacts
- FBI contacts
- Local fire department
- Local FAA contact
- Local TSA contact
- Tenant contacts

It is essential that first responders and airport management have the capability to communicate. Where possible, coordinate radio communication and establish common frequencies and procedures to establish a radio communications network with local law enforcement.

Airport Tenant Facilities

Tenant access controls to their leasehold properties should be incorporated into the airport's security procedures and/or alarm and reporting system. Airport management must coordinate with the airports tenants to ensure that security procedures or systems used by those tenants do not conflict or leave coverage gaps. For example, airport management should coordinate and ensure security procedures exist and are harmonized with maintenance facilities that have access to both the public side of the fence and the aircraft parking and movement areas.

Aircraft and Vehicle Fueling Facilities

For obvious reasons, fueling facilities are potentially 'high threat' areas and movement should be controlled in these areas with fencing, lighting and access controls whenever possible. Trucks used to transfer fuel to aircraft should be secured when not in use. This includes controlling fuel truck keys and not leaving keys in trucks while unattended. Parked fuel trucks should be in an easily monitored location.

➤ ➤ ➤

CHAPTER III

EXAMPLES OF AIRPORT SECURITY SECTIONS AND ISSUES TO BE CONSIDERED

The following pages provide specific examples of security programs that may be helpful in developing each airport's individualized security program:

Attachment 1: Airport Watch Program

Attachment 2: Measures to be Implemented Based on Threat Advisory Level

Attachment 3: Rules and Regulations Needed to Support General Aviation
Security

Attachment 4: Airport Security Responsibilities

Attachment 5: Airport Lessee/Tenant/Employee Security Responsibilities

ATTACHMENT 1

(EXAMPLE)

AIRPORT WATCH PROGRAM

The main objective of an Airport Watch Program is to help eliminate crime on and around the airport and bring all suspicious activity to the attention of law enforcement officers so that appropriate action can be taken. In the event that any person looks suspicious, all tenants and users are asked to contact airport management or airport police.

1. SECURITY PROCEDURES TO BE FOLLOWED

- a. Ensure all gates entering the AOA are closed and locked (or manned) at all times.
- b. Maintain a continuous visual surveillance of the airport
- c. Report all suspicious activity
- d. Challenge and ask for proper identification of all pedestrians and vehicles within the AOA
- e. Monitor/escort unauthorized personnel

2. TYPES OF SUSPICIOUS ACTIVITY TO BE ON THE LOOKOUT FOR

- a. Aircraft with unusual or unauthorized modifications
- b. Persons loitering for extended periods in the vicinity of parked aircraft or in the AOA
- c. Pilots who appear to be under the control of other persons
- d. Persons wishing to obtain aircraft without presenting proper credentials or persons who present apparently valid credentials but do not have a corresponding level of aviation knowledge
- e. Individuals wandering around the airfield after hours or persons on the airfield with no identification
- f. Anything that doesn't look right (i.e. events or circumstances which do not fit the pattern of normal lawful activity at the airport)

3. AIRPORT SIGNAGE

- a. **Airport Watch signs:** These signs will be posted along the landside areas of the airport
- b. **Authorized Pedestrian Traffic Only signs:** These signs will be posted at all pedestrian gates
- c. **Authorized Vehicular Traffic Only signs:** These signs will be posted at all gates leading to the airfield where vehicular traffic is allowed
- d. **Gate Caution signs:** These signs will be posted at all vehicular gates informing drivers that only one vehicle may pass per gate opening

ATTACHMENT 2

(EXAMPLE)

MEASURES TO BE IMPLEMENTED BASED ON NATIONAL THREAT LEVEL

LOW RISK (GREEN)

Airport Management Measures

- Notify airport employees, tenants, etc. possessing an operational need to know of the HSAS Threat Level
- Review and implement applicable emergency plans
- Close and lock all access points accessible to the general public during non-operational hours
- Establish random landside and airside security patrols

Tenant Measures

- Notify sub-tenants of security measures applicable to this level
- Close and lock all airside/AOA access points during non-operational hours
- Immediately report any suspicious airport activity to the police or airport management

GUARDED RISK (BLUE)

Airport Management Measures

- Notify airport employees, tenants, etc. possessing an operational need to know of the HSAS Threat Level
- Review and implement applicable emergency plans
- Close and lock all access points accessible to the general public during non-operational hours
- Conduct random landside and airside security patrols

Tenant Measures

- Notify sub-tenants of increased security measures applicable to this level
- Close and lock all airside/AOA access points during non-operational hours
- Immediately report any suspicious airport activity to the police or airport management

ELEVATED RISK (YELLOW)

Airport Management Measures

- Notify airport employees, tenants, etc. possessing an operational need to know of the HSAS Threat Level
- Review and implement applicable emergency plans
- Close and lock all access points accessible to the general public during non-operational hours
- Conduct frequent random landside and airside security patrols

Tenant Measures

- Notify sub-tenants of increased security measures applicable to this level
- Close and lock all airside/AOA access points during non-operational hours
- Closely monitor general public access to the airside/AOA
- Maintain increased surveillance over the leased airside ramp areas
- Immediately report any suspicious airport activity to the police or airport management

HIGH RISK (ORANGE)

Airport Management Measures

- Notify airport employees, tenants, etc. possessing an operational need to know of the HSAS Threat Level
- Review and implement applicable emergency plans
- Close all vehicular access points to the AOA. Access shall be by code/key card entry only to those pre-approved for AOA access
- Notify and instruct all airfield tenants to limit pedestrian access to the AOA and ramp areas to only those individuals that have legitimate entry requirements
- Implement a Ramp Access Placard Program and restrict vehicle access to AOA, flight ramps and aprons to only those vehicles possessing a valid placard
- Conduct frequent random landside and airside security patrols

Tenant Measures

- Notify sub-tenants of increased security measures applicable to this level
- Closely monitor general public access to the airside/AOA
- Restrict vehicle access to AOA, flight ramps and aprons to only those vehicles possessing a valid Ramp Access Placard
- Maintain a constant surveillance over the leased airside ramp areas.
- Close and lock all personnel and vehicular access points to the AOA after working hours.

- Immediately report any suspicious airport activity to airport management or the police

SEVERE RISK (RED)

Airport Management Measures

- Notify airport employees, tenants, etc. possessing an operational need to know of the HSAS Threat Level
- Review and implement applicable emergency plans
- Implement a Ramp Access Placard Program and restrict vehicle access to AOA, flight ramps, and aprons to only those vehicles possessing a valid Ramp Access Placard
- Close all vehicular access points to the AOA. Access shall be by code/key card entry only to those pre-approved for AOA access
- Notify and instruct all airfield tenants to restrict access to the AOA and ramp areas to only essential personnel
- Conduct random inspections of vehicles and aircraft within the AOA
- Coordinate and schedule random security checks of personnel within the AOA
- Randomly deploy additional security patrols including Law Enforcement Officers to provide extra surveillance on the airport property
- Reduce the number of access points to the AOA and ramp areas to an absolute minimum
- Increase the presence of airport employees and police on and around the airport

Tenant Measures

- Restrict access to the AOA and ramp areas to only essential personnel and vehicles
- Challenge and positively identify all persons entering the AOA
- Close and lock all nonessential access points to the AOA and ramp areas
- Immediately report any suspicious airport activity to the airport management or police department (911)
- Restrict vehicle access to the AOA, flight ramps, and aprons to only those vehicles possessing a valid Ramp Access Placard
- Tenants must escort vehicles that do not display a Ramp Access Placard
- Verify continuous 5-year employment history background of all employees, i.e. driver licenses, addresses, and other pertinent information deemed appropriate

✈ ✈ ✈

ATTACHMENT 3

(EXAMPLE)

**RULES AND REGULATIONS NEEDED TO SUPPORT
GENERAL AVIATION SECURITY**

SECTION 1 - Applicability of Rules and Regulations

All persons on, and users of, the airport shall comply with and be governed by these Rules and Regulations.

Compliance

- (a) The use of and entry upon the airport shall create an obligation on the part of the user to comply with these Rules and Regulations. Any permission granted by the Airport Director to a person, directly or indirectly, expressly or by implication, to enter upon or use the airport, is conditioned upon compliance with these Rules and Regulations and the payment of any fees or charges to the City (County) for the use of the airport or any facility located thereon.
- (b) It shall be unlawful for any person to do or commit any act forbidden herein or to fail to perform any act required by these Rules and Regulations or to fail to pay any administrative fees or fines established by these Rules and Regulations.

Other Laws

All applicable provisions of the laws of the United States, Federal Aviation Regulations, laws of the State of Florida, laws of the City (County) of _____, and other ordinances, now in existence or hereafter enacted, shall be in effect at the airport. All applicable provisions of pertinent regulations promulgated by the City (County) affecting the operation of the airport not in conflict with these Rules and Regulations, now in existence or hereafter enacted, shall be in effect at the airport.

Enforcement

These Rules and Regulations, as well as all applicable state laws and City (County) ordinances, shall be enforced at the Airport Director, and other law enforcement officers whose jurisdiction lies herein.

Fines and Penalties

Violators of these Rules and Regulations shall subject such person and/or tenant to damages equal to the following:

- (a) First Offense - \$_____ fine per offense per day until such violation is remedied.
- (b) Second Offense - \$_____ per offense per day until such violation is remedied, if same is a previously documented offense within the past twelve (12) months.
- (c) Subsequent Offenses - \$_____ per offense per day until such violation is remedied, if same offense has twice been previously documented within the past twelve (12) months. This will also likely result in permanent disbarment from the airport.

Violations of these Rules and Regulations shall constitute a second-degree misdemeanor and may include additional fines not to exceed \$500 per violation and/or imprisonment for a period not to exceed sixty (60) days for each violation as well as payment of all costs and expenses incurred in prosecuting the offense. In addition, violators shall be subject to all civil penalties as may be provided herein. The provisions set forth in this section are additional and supplemental penalties. Nothing in this section shall prevent the City (County) from enforcing these Rules and Regulations by any other means allowed by the law.

In addition to any misdemeanor penalties set forth in the prior paragraph, the Airport Director may remove any person from the airport who knowingly and willfully violates any of these rules and/or Operational Directive, and may deny use of the airport to such person (including, but not limited to requesting that the Council terminate any lease for facilities at the airport) if the Airport Director determines that such denial is necessary under the circumstances. The Airport Director may take such other measures as may be permitted by law to enforce these Rules and Regulations and maintain the City's control, and the safe operation, of the airport, including but not limited to issuing warning letters and publishing the names of persons who have been issued such warning letters. Any person aggrieved by a decision of the Airport Director removing such person from the airport or denying the use of the airport to such person pursuant to this section may appeal such decision to the City (County) Council. If the Airport Director determines that such violation(s) presents a threat to the public, health, safety, or welfare, such right of access shall be suspended pending completion of such appeal.

Violators may also be charged an amount equal to any civil fine imposed by any agency upon the City (County), as a result of the violation and/or fines or penalties may be assessed against the tenant responsible for such fines and/or penalties. Additionally, offenders may be subject to a charge of \$1,000.00 per occurrence – not as a penalty, but as liquidated damages for fines or administrative cost incurred by the City (County) as a result of the violation.

Appeal of Penalties

Any person wishing to appeal any violation of these Rules and Regulations (including Security Violations outlined in Section 2) shall have the opportunity to present their case

to the City (County) Council, who will be the final governing body and who will make an ultimate decision to enforce, forgive, reduce, and/or eliminate the penalty.

Severability

If any provision of these Rules and Regulations or the application thereof to any person or circumstance is held invalid, the remainder of these Rules and Regulations shall not be affected.

SECTION 2 – Airport Security Program

Entry to Airport Operating Area (AOA) or Other Restricted Areas

No person shall enter the AOA or other Restricted Area of the airport except persons who enter in accordance with this Security Program outlined herein unless otherwise authorized, in writing, by the Airport Director.

Security Devices and Directives

No person shall in any way tamper or interfere with a lock or closing mechanism of any door or gate leading to the AOA or other Restricted Area, nor shall any person otherwise knowingly breach, disobey or disregard any Security Program, directive or plan at the airport.

Intentional Security Violation

Any person who knowingly or intentionally enters or allows another person to enter any Restricted Area without proper authorization by any use of any key, gate card, identification badge, vehicle permit, or other such instrument shall immediately - and may permanently - be denied access to the airport and shall, in addition to other penalties outlined in these Rules and Regulations, be required to immediately relinquish such instrument to the City (County). **There is a Zero Tolerance policy on intentional security violations.**

Security Violations

In addition to other remedies, and/or penalties, violation of this Security Program shall subject such person or tenant to damages equal to the following:

- (a) First Offense - \$_____ fine per offense per day until such violation is remedied.
- (b) Second Offense - \$_____ per offense per day until such violation is remedied, if same is a previously documented offense within the past twenty-four (24) months.

- (c) Subsequent offenses - \$_____ per offense per day until such violation is remedied, if same offense has twice been previously documented within the past twenty-four (24) months. This will likely result in permanent disbarment from the airport.

In addition to the above-listed fines, violators may be charged an amount equal to any civil fine imposed by any agency upon the City (County) as a result of the violation and/or fines or penalties may be assessed against tenant's airport operating license. Additionally, offenders may be subject to a charge of \$1,000.00 per occurrence – not as a penalty, but as liquidated damages for fines or administrative cost incurred by the City (County) as a result of the violation.

Tenant Responsibilities

Each tenant shall comply with the following:

- (a) Each tenant shall be responsible for making these Rules and Regulations available to its customers, guests, and/or invitees by maintaining a copy of these rules on the premises.
- (b) Each tenant shall be responsible for controlling access through their leased premises to the AOA or any other Restricted Area. Failure to comply will result in penalties outlined herein.
- (c) Each tenant shall submit a current copy of their normal business hours to the Airport Director's Office. During these normal business hours, each tenant or business shall escort each visitor or guest who requires access to the AOA or other Restricted Area unless such visitor or guest has authorized access to such areas pursuant to these Rules.
- (d) Each tenant shall provide completed "*Airport Employee Identification Form(s)*" (*sample attached in the Appendix*) to the Airport Director's Office for each person employed by the tenant. Each tenant is responsible to ensure that these forms are maintained in a current status.
- (e) **If and/or when such action is mandated by either the Transportation Security Administration (TSA) or the City (County) Council**, each tenant located on the airport and each business licensed to do business at the airport that requires access to the AOA or any Restricted Area for conduct of its business:
 - (i) Shall conduct, or cause to be conducted, a Security Background Check on each of its current employees with the access to the AOA, SIDA, aircraft parking areas, or other Restricted Area and

- (ii) Shall submit to the Airport Director a list of all such employees and the results of the employees' criminal records check if required by the security background check

- (f) Each person over the age of sixteen (16) on airport property is required to carry at least one government issued identification card (driver's license, military or state issued id, passport, etc).

Badge Program

All persons requiring access to or physically within the AOA or other Restricted Areas must display his/her identification badge in these areas of the airport. Failure to do so shall constitute a violation of the Airport Security Program by the person so violating and possibly, if such person gained access through a tenant's property, by the tenant. This **does not** apply to pilots, students, or passengers inside of an aircraft.

Vehicles

The operator of each vehicle requiring access to the *any* areas where aircraft are parked, the AOA, or the SIDA, shall be required to obtain a vehicle access permit from the office of the Airport Director. Unless the vehicle is at all times operated under the escort of a tenant, each vehicle owner shall be required to provide the following to obtain the vehicle access permit.

- (a) A current copy of the vehicle insurance policy. Vehicles requiring access to the AOA shall maintain liability limits as required by the City (County) Rules and Regulations.
- (b) Provide a letter from their sponsoring tenant or club documenting the need for vehicle access.
- (c) Sign a statement acknowledging an understanding of these Rules and Regulations and the operators agreement to comply with these Rules and Regulations.

These Rules and Regulations have been approved by Resolution No. _____ of _____ City (County), on _____.

✈ ✈ ✈

ATTACHMENT 4

(EXAMPLE)

AIRPORT SECURITY RESPONSIBILITIES

Perimeter Security

- The airport shall be responsible for ensuring that the airfield perimeter fence consisting of 6' chain link with an additional 1' of barbed wire or large screening hedge is in place to secure the airside facilities from the landside
- No unauthorized person shall in any way tamper or interfere with airport perimeter fence, vehicular gate access system, or pedestrian gates
- The airport shall be responsible for maintaining all vehicle and pedestrian access gates installed by the city/county
- The airport shall patrol the perimeter fence regularly to ensure that electric gates are functioning properly, pedestrian gates remain closed and locked, and the fence system has not been compromised

Airport Signs

- Adequate no trespassing signs shall be installed along the perimeter fencing
- All vehicular and pedestrian access gates shall have appropriate signs
- Signs shall be placed around the airfield to delineate the boundary of tower controlled movement areas
- Clearly post emergency telephone numbers (police, fire, FBI, airport management, etc.) so that people may report suspicious activity
- Place a prominent sign near areas of public access warning against tampering with or unauthorized use of aircraft
- Use signage to control airside area access
- Install signs to direct the movement of people and inform patrons of pertinent information regarding the safe and efficient use and operation of the facility. This may include, but is not limited to, parking and directional signs, informational signs, do-not-enter signs, warning signs, etc. Whatever the sign type, it should communicate the proper message to the appropriate party at the right time and place

- Develop a Security Mission Statement with the help of the Airport Security Committee (ASC). Display the statement in an appropriate location(s). Make the sign large and visible to customers, guests, and potential threats

Notification

- The airport shall maintain a current directory listing of tenants
- The directory shall be published for distribution on a bi-annual basis
- A fax list of airport tenants will be maintained for timely dissemination of Security Notices

Patrols of the Airport

- Patrols of the airport shall take place 24 hours a day, 7 days a week.
- Airport operations and security are responsible for monitoring the airport runway and taxiway areas and facilities to ensure the safety and security for the benefit of the flying and traveling public

Access to the Airside Facilities

- The airport shall issue identification badges to persons identified by lessees as being authorized to access the airside facilities of the airport
- Codes to pedestrian gates shall be changed on at least an annual basis or when the lessee requests
- Guests and passengers shall be escorted and remain within eyesight of authorized personnel
- Based/Transient/Student pilots shall be able to use their pilot's license as identifications and not be required to have a badge
- Close vehicular and pedestrian gates leading into the airside area and lock them when not in use
- Restrict pedestrian and vehicular access into the airside area to as few locations as possible, balancing the need for authorized access by emergency, safety and maintenance personnel, and aircraft owners and users, inside and outside the airside area
- If not escorted to the aircraft, visually follow the crew and passengers from the lobby to the aircraft and immediately report any deviations

- Periodically change access codes and locks to vehicular and pedestrian gates leading into the airside area
- Install security fencing as appropriate to protect against inadvertent or unauthorized access to the airside area. Until such time as the entire airside area is enclosed, priority should be given to areas where easy public access to the airside area is of most concern

Monitoring and Protecting Airport Users and Property

- Doors on aircraft storage hangars should be kept locked at all times when not in use. Conduct scheduled and random hangar inspections
- Airports and tenants should install sufficient lighting equipment to illuminate buildings, walkways, aircraft ramps, and aprons
- Monitor airport property by performing regular inspections, and by means of guard, alarm systems, video surveillance or intrusion detection equipment, if warranted
- Consider security patrols for ramp and aircraft parking areas, particularly during periods of heightened security alerts
- Request periodic inspections or patrols of the airport by local law enforcement officers. If warranted, consider employing local law enforcement officers on a regular or part-time basis
- Install locks on airfield electrical vaults and other electrical systems, including (non-FAA) NAVAIDS
- Store equipment in a secure location when not in use
- If feasible, provide 24/7 FBO service
- Secure refueling trucks and fuel farms
- Install barriers to protect fueling facilities, hazardous material storage areas, and other areas of concern
- Install locks on fuel cabinets, fill hatches and pumps, and electrical cabinets of fueling facilities. Do not lock emergency shut-off valves

Identification

- Use identification (ID) media (badges, etc.) for allowing access to anyone needing to enter the airside area and for controlling the movement of persons within the

airside area. Temporary passes and sign-in log can be used for transients and visitors, as well as pilots license, where appropriate

- Any person authorized to enter the airside area or move within the airside area shall display a standard ID badge with sufficient information to clearly identify the individual and ascertain the level of security authorization
- Issue airport identification credentials to all airport employees tenants and contractors
- All employees, tenants and contractors with access to aircraft must wear proper identification when on the ramp
- Implement procedures for challenging persons who are not displaying proper identification and incorporate into Airport Security Plan
- Any one without proper identification should be escorted at all times while in restricted areas of the airside area by authorized personnel
- Identification media should have an expiration date as a control measure. In addition, expired ID's should be deactivated from any electronic access systems
- Use credential checking for crews and passengers by a qualified individual
- Require flight crew to verify the identity of their passengers prior to entering the airside area
- Verify the identity of individuals renting or purchasing an aircraft or joining a flying club by checking government-issued photo ID
- Know employees and customers. Establish procedures to screen passengers and/or cargo

General Aviation Security Information

- What airport management, tenants, and users should be looking for:
 - Aircraft with unusual or unauthorized modifications or markings
 - Unscheduled visits by consultants, contractors, utility workers, surveyors who need access to airside facilities
 - Persons or vehicles loitering for extended periods in the vicinity of the airport, parked aircraft or in the airside area
 - Pilots who appear to be under the control of other persons

- Persons with above average interest in aircraft and their performance capabilities
- Persons wishing to obtain aircraft without presenting proper credentials
- Persons who present apparently valid credentials but do not have a corresponding level of aviation knowledge
- Dangerous or deadly weapons or explosives being loaded onto an aircraft
- Any person who makes threats or statements inconsistent with normal uses of aircraft
- Stolen or missing aircraft
- Anything that appears unusual or does not fit the pattern of lawful, normal activity at the airport

✈ ✈ ✈

ATTACHMENT 5

(EXAMPLE)

AIRPORT LESSEE/TENANT/EMPLOYEE SECURITY RESPONSIBILITIES

Lessee Responsibilities

The Lessee is responsible for the security and protection of their leased premises, any improvements thereon, its equipment and property on the airport.

Hangars, Buildings, and Ramps

- Airport tenants shall keep all vehicles, personnel gates, doors and other means of ingress and egress to the airport secured or controlled at all times to prevent the access of unauthorized persons
- Airport tenants and their employees shall be responsible for control and prevention of unauthorized access to the airside of their facilities or the leasehold areas of other tenants
- Airport tenants and employees shall monitor pilots, crews, passengers, and aircraft on the ground and be responsible for matching specific crew to specific aircraft, both based and transient
- Airport tenants and their employees shall be responsible for escorting passengers and guests on the airside of the airport
- The pilot in command (PIC) shall have the responsibility to ensure that the identity of all occupants is verified and all baggage/cargo is known to occupants

Aircraft

- Aircraft shall be secured by locking the aircraft in a hangar or by some type of physical locking or disabling device when unattended. The following is a list of devices that meet this requirement:
 - Throttle locks
 - Chock locks
 - High security door locks
 - Wheel boots
 - Propeller locks
- Additional methods for securing aircraft can include using security tape on aircraft doors and visually inspecting aircraft prior to departure

Vehicle and Pedestrian Access

- All vehicles allowed on the airside of the airport shall display a valid Ramp Permit sticker and guests shall be escorted in compliance with the Ramp Driving Guidelines Manual (if available)
- Only authorized personnel and tenants shall be given access to vehicle and pedestrian gates
- No unnecessary cars, limousines, taxis, rental cars, vendor, or delivery vehicles will be allowed on the ramp

Fuel Farms and Trucks

- All fuel farms should be contained within a fenced area to restrict access
- Locks should be installed on fuel cabinets, fill hatches, sumps, pumps, and electrical cabinets to reduce the risk of tampering
- Fuel farms should be monitored 24 hours per day preferably by video monitoring capability
- Fuel trucks shall be locked when not in use and parked away from structures and perimeter fencing in a location that can be easily monitored by FBO employees

Refer to the appropriate section of the NFPA code before locking components on the fuel truck or fuel farm

Flight Training/Aircraft Rental

- Conduct student/renter pilot screening, as appropriate
- Have company employees retain possession of aircraft keys until a company representative approves the individual
- Restrict student/renter pilots access to ramp areas

Flight Operations

- Monitor pilots, crews, passengers and aircraft on the ground
- Establish procedures for matching specific crew to specific aircraft, both based and transient. This could be done by issuing a code presented when they arrive/depart the airport. This may be different based on the airport's location, size, and proximity to sensitive areas

- Prior to entering the airside area, the PIC should ensure that the identity of all passengers are verified, all passengers are at the invitation of the owner/operator, and that all baggage and cargo is known to the passengers
- Use passenger screening, as appropriate
- For any changes in the passenger manifest, request written notification from the company or individual chartering the aircraft
- Charters being booked by previously unknown clients warrant a thorough reference check of those that will be flying in the aircraft. This could include charter companies they have conducted business with in the past. This may require some lead-time to ensure a thorough check can be conducted before the charter date
- Pilots are reminded to receive an up-to-date briefing on the status of special flight restrictions at all times

Agricultural Operations

- Tie-down aircraft with chains and locks, rather than ropes
- Prop-lock the aircraft with high strength chain and lock
- Removal of aircraft battery after flight
- Install throttle lock
- Personal recognition of company employees and owners
- Check in with airport operator prior to daily activity
- Restrict activity to daylight operations only

Glider/Sailplane Operations

- Ensure companies escort all trainees and customers for orientation flights
- Personal recognition of company employees and owners
- Ensure customers are confined to a hold area under company supervision
- Install throttle locks on tow aircraft
- Check in with airport operator prior to daily operations

- Restrict activity to daylight operations only

Skydiving Operations

- Install aircraft throttle locks on the jump aircraft
- For larger jump aircraft, insure cockpit door is closed and locked at all times while skydivers occupy the cabin of the aircraft
- Ensure no student or qualified skydiver is authorized access to the aircraft without escort
- Ensure all manifested skydivers have had an identification check prior to boarding the jump aircraft
- Company personnel required to escort all manifested skydivers to the aircraft
- Ensure a qualified jumpmaster is aboard the aircraft in the cabin at all times prior to the exiting of the aircraft
- Verify after the landing of the skydiver, that all persons are accounted for as listed on the boarding manifest
- Restrict all operations to daylight operation

Aerobatic Operations

- Install throttle locks on the aircraft
- Ensure only wavered crewmembers by the FAA utilize the aerobatic box through personal recognition
- Ensure prior approval of the FAA and airport operator prior to use of the established aerobatic box or clear air activity for training
- Ensure prior coordination with airport operator and airport businesses has been coordinated prior to flight and appropriate announcements are accomplished on the established UNICOM frequency
- Restrict aerobatic activity to daylight operations only

Ultra-light Aircraft Operations

- Ultra-light operators must be registered with the airport management

- Ultra-light operators must be familiar with the airport's flight patterns, local restrictions and rules
- Based ultra-light aircraft must be secured when not in use

Banner Tow Operations

- A permit from the airport management is required, with list of all employees requiring access to the banner pick-up/drop area
- Ensure that all pilots are certified for banner tow operations
- Check in with airport operator, prior to set up of daily operations
- Ensure that only company employees are allowed in the 'banner tow' area

Commercial Filming

- A permit from the airport management is required, with list of all employees requiring access to the airport
- Security for film-shoot is required
- Single point of access to site controlled by a Law Enforcement Officer
- For AOA filming, an airport safety officer must be present at all times
- For leasehold filming, a leasehold safety officer must be present at all times
- A single person point of contact from the production company must be on site at all times
- Clearances for all types of activities must be secured from airport management

Outside Vendors

- A permit from airport management is required, with list of employees, and proper identification displayed while on the airport. Evidence of insurance is required.
- Vendors are restricted to defined areas only
- Vendors must be escorted by FBO personnel while on their ramp

Military

- Military identification system should be coordinated with airport management

- Military personnel must be trained on movement on the AOA
- Clearly defined areas of operations must be developed to avoid confrontation during heightened alert status

Large Aircraft-Transport Category That Qualify As Weapons Of Mass Destruction (WMD)

Active aircraft:

- Aircraft should be parked to make it difficult for theft: aircraft parked nose-in, vehicles or ground equipment parked to block aircraft, tow bars removed and secured, stairs, work stands, tugs and power (start) carts parked remotely to aircraft, etc.
- Aircraft should be disabled for flight until needed
- Fueling operations are to be done prior to flight, not upon arrival
- Emergency notification phone numbers must be provided to airport management
- Additional security placed on aircraft around the clock or other devices that would secure aircraft, in the form of guards, proximity devices, alarms, etc.
- Leasehold or airport ID for all parties allowed at aircraft site
- All passengers and crew escorted to the aircraft by the FBO
- Use of password issues by FBO is encouraged

Stored aircraft:

- Upon arrival at airport, aircraft must be disabled
- Emergency notification phone numbers must be provided to airport management
- A timeline for removal of aircraft must be established
- Additional security shall be placed on aircraft around the clock or other devices that would secure the aircraft
- Leasehold or Permit ID for all parties allowed at aircraft site

- Refer to TSA document "Security Programs for Aircraft 12,500 Pounds or More"
A copy of the full documents can be found at:
<http://www.dot.gov/documents/12500lbs.pdf>.

✈ ✈ ✈

CHAPTER IV

THE MODEL PLAN

The preceding chapters discussed why each airport in Florida needs a security plan and what needs to be included in a plan. Chapter Four is a model to be used in preparing each airport's plan. FAC will send an electronic version of the plan to any interested airports for their use.

This generic model is provided as a starting point for each general aviation airport in Florida. Each airport manager and security team should determine how to customize the plan to fit the specific needs of that particular airport.

The Transportation Security Administration wanted to see a standardized security program around the country and this model plan will help Florida's airports with a statewide standard, as well.

An airport manager member of the Florida Airports Council will be asked to serve as a regional representative in each FDOT district that you may call upon with questions, or to provide you assistance regarding general aviation security in the future.

The FAC web page now has a section dedicated to general aviation security and these regional representatives will be posted on that site.

If you have any questions regarding this model plan, please feel free to contact FAC's Executive Director at the following address:

Bill Johnson, AAE
Executive Director
Florida Airports Council
1801 North Meridian Road, Suite C
Tallahassee, FL 32303
Tel: (850) 224-2964
Fax: (850) 681-6185
E-mail: bill@floridaairports.org

Note: After August 15, 2004, FAC's new address will be:

2100 Delta Way, Suite 2
Tallahassee, FL 32303



*Restricted Information
Not for Public Dissemination
(331.22 F.S.)*

**Security Plan
For
(*Airport Name*)**

(Original Publication Date)
(Date Last Revised)

Table of Contents

<u>Section</u>	<u>Page No.</u>
Section I: Disclosure Statement/Security Responsibilities.....	<i>(fill in)</i>
Section II: General Information.....	
Section III: Definitions and Terms.....	
Section IV: Administration.....	
Section V: Aircraft Movement Area/Security Control.....	
Section VI: Airport Security Procedures.....	
Section VII: Airport Emergency Grid Map.....	
Section VIII: Identification of Airport Personnel.....	
Section IX: Identification of Vehicles.....	
Section X: Law Enforcement.....	
Section XI: Special Events.....	
Section XII: Increased Security Threats.....	
Section XIII: Aviation Security Contingency Plans.....	
Section XIV: Model Forms.....	

Section 1: Disclosure Statement/Security Responsibilities

(Distribution of these Security Procedures should be restricted to individuals with a legitimate need for access to them. Each recipient of the manual should be noted, as well as the airport management representative responsible for the plan. For example:)

This manual has been assigned to:

Name:

Title:

Representing:

Telephone:

Office:

Home:

Cell:

Emergency:

Fax:

E-mail:

Information regarding this manual should be directed to:

Name:

Title:

Representing:

Telephone:

Office:

Home:

Cell:

Emergency:

Fax:

E-Mail:

Section II: General Information

(Provide the following information to fit the needs of your airport. A collaborative effort among airport management, public safety officials, tenants, and users may result in a superior document that has the necessary buy-in from all participating individuals, agencies, and private companies)

1. Forward

Identify the airport owner and the person(s) responsible for airport activities – e.g. state, county, authority, commission

2. Introduction and Purpose

Provide a brief introduction that describes the purpose and the need for a security plan

3. Distribution

Provide a list of all individuals and agencies that will receive copies of the airport security plan

4. Name/Location of Airport

Include items such as:

- a. Airport name*
- b. Airport address*
- c. Normal business/24 hour emergency/fax phone numbers*
- d. Airport identifier*
- e. Proximity to nearest major city*
- f. Airport geographical coordinates*

5. Airport Activities

Include items such as:

- a. Types of flight activities (e.g. flight school, corporate, etc.)*
- b. Hours of operation*
- c. Number of annual of operations*
- d. Number of based aircraft*

6. Airport Description

Include items such as:

- a. *Size: Acres*
- b. *Runways, Taxiways, Ramps: Identify Runways and their dimensions, taxiways, and ramp areas. Provide an airport layout plan/diagram as an attachment.*
- c. *Buildings:*
 - i. *List the number and types of buildings (offices, hangars, maintenance shops).*
 - ii. *List the primary tenants for each building*
- d. *Airport Tenants:*
 - i. *List hours of operation*
 - ii. *List primary and emergency contact information*
- e. *Other Airport Facilities*

7. Emergency Telephone Numbers

List all appropriate emergency contact numbers. Include point of contact names and office hours of operation as appropriate

- a. *All Emergencies.....911*
- b. *State Police (non-emergency)*
- c. *Local Police (non-emergency)*
- d. *Local Fire Department*
- e. *Airport Director (24 hour contact)*
- f. *Airport Facility Manager*
- g. *FDOT Aviation Office.....850-414-4500*
- h. *FDOT District Aviation Representative*
- i. *FBI Local Field Office*
- j. *FAA Flight Standards District Office (FSDO)*
- k. *TSA Airport Watch Hot-Line.....866-427-3287*
- l. *Local TSA Federal Security Director*
- m. *Other*

Section III: Definitions and Terms

(The following definitions and terms were provided by the FAC Technical Committee and are examples only. Your airport may elect to use any or all of these definitions in your Manual, if you feel it they are appropriate.)

Definitions

The following words, terms and phrases when used herein shall have the meanings described. Words which relate to aeronautical practices, processes and equipment, not defined herein, shall be construed according to the definitions in Florida Statutes Chapter 332 or, if not defined therein, according to their general usage in the aviation industry.

— — — — —

“Advisory Circular” shall mean the FAA’s Advisory Circular No. 150/5300-13, published September 29, 1989 entitled “Airport Design” including all amendments.

“Aircraft Approach Category” shall mean one of five categories of aircraft, symbolized by the letters A through E, as such categorization is used in the Advisory Circular. The grouping is based on the stalling speed of aircraft in their landing configuration at their maximum certificated weight.

“Aircraft Rescue Fire Fighting” or “ARFF” shall mean the organization of those persons meeting the performance criteria for airport fire fighters set forth in NFPA 1003, “Standard for Professional Qualifications for Airport Fire Fighters” and having the basic knowledge, skills, and abilities identified in NFPA 1001, “Standard for Fire Fighter Professional Qualifications.” In the event that the airport does not have a dedicated ARFF facility, the term shall refer to such fire fighting facility that has been designed by the Airport Director or other appropriate authorized official to respond to fire and other emergencies on the airport.

“Airplane Design Group” shall mean a six member grouping of aircraft, symbolized by the roman numerals I through VI, as such categorization is used in the Advisory Circular. The grouping is based on the wingspan of the aircraft.

“Airport” Shall mean the _____ Airport including all properties therein.

“Airport Minimum Standards for Aeronautical Activities” shall mean the city (county) policy document (if any), setting forth the minimum standards for aeronautical activities at the airport (as such term is defined therein), as such policy may be amended from time to time. To the extent of any conflicts between that policy statement and these Rules and Regulations, these Rules and Regulations shall prevail.

“Airport Director” shall mean the representative of the city (county), or designee, with the powers to direct all matters at the airport, to supervise all activities at the airport, to be

responsible for the operation, management and maintenance of the Airport and to enforce these regulations.

“Airport Operations Area” or “AOA” shall mean any area of the airport identified by the Airport Director and/or used or intended to be used for landing, taking-off or surface maneuvering of an aircraft as depicted on a map maintained on file in the office of the Airport Director but shall not include apron or ramp areas normally leased by tenants for their exclusive use.

“Airport Vehicle” shall mean any vehicle owned or operated by the airport administration.

“Apron” or “Ramp” shall mean those areas of the airport designated by the Airport Director for the loading or unloading of cargo or passengers, servicing, or parking of aircraft.

“ARC” shall mean Airport Reference Code, a two-component coding system where the first component, depicted by a letter, is the Aircraft Approach Category, and the second component, depicted by a Roman numeral, is the Airplane Design Group.

“ASDA” shall mean the accelerate-stop distance available, as such term is used in Advisory Circular 150/5300-13 as may be amended and/or any other such official document published by the FAA.

“Authorized Person” shall mean any person with the explicit permission of the Airport Director or his/her designee. All Authorized Personnel shall carry in their possession a valid airport issued identification badge.

“Club Aircraft” shall mean aircraft owned by a flying club but shall not mean an aircraft managed as part of a fractional ownership program as defined in the Federal Aviation Regulations.

“City” shall mean City of _____, a municipal corporation existing under the laws of the State of Florida.

“City Code” shall mean the Code of Laws and Ordinances of _____, Florida, as may be amended from time to time.

“Council” shall mean the _____ City Council.

“County” shall mean County of _____, Florida.

“Courtesy Vehicle” shall mean any vehicle, other than a taxicab, used to transport persons, baggage or goods, or any combination thereof, between the airport and the business establishment owning or operating such vehicle, the operation of which is generally performed as a service without direct costs to the passenger.

“Declared Distance” shall mean the distances available for an airplane’s takeoff run, takeoff distance, accelerate-stop distance, and landing distance requirements.

“Emergency Vehicle” shall mean any fire department, police, ambulance, airport, federal, military, or any other such vehicle designated by the Airport Director, police/sheriff’s department, county department of emergency services, or any other state or federal agency as an authorized emergency vehicle.

“Escort” shall mean for a person who has access authority to the AOA or other Restricted Area to accompany and maintain direct control over the activities of a person without such authority.

“FAA” shall mean the United States Department of Transportation Federal Aviation Administration or any successor federal agency thereto.

“Federal Aviation Regulations” shall mean the regulations of the United States Department of Transportation’s Federal Aviation Administration as codified at Title 14 C.F.R. as currently in effect or as hereafter amended.

“Flying Club” shall mean any group of persons owning one or more aircraft and intending to operate the aircraft for noncommercial purposes but shall not mean any entity that manages aircraft as part of a fractional ownership program, as defined by the Federal Aviation Regulations.

“Jet Aircraft” shall mean aircraft powered by turbine or any other engines where thrust is not provided by an external propeller.

“LDA” shall mean landing distance available, as such term is used in Advisory Circular 150/5300-13 as may be amended and/or any other such official document published by FAA.

“Maintenance Run-up” shall mean the operation of the engines on an aircraft for any purpose other than for proceeding expeditiously to and from the airport runway system for takeoff, landing, or taxiing to and from an approved run-up location.

“National Fire Protection Association” or **“NFPA”** shall mean all codes and standards contained in the Standards of the National Fire Protection Association, as the same may be amended from time to time.

“Non-operating Aircraft” shall mean any aircraft located on the airport which does not possess a *current* certificate of airworthiness (having all required inspections, maintenance, etc.) issued by the FAA and is not actively being repaired.

“Operational Directive” shall mean a written order issued by the Airport Director or his/her designee bearing the designation “Operational Directive” and requiring specific

operational procedures or prohibiting specific operational procedures or prohibiting specific operations or types of operations on the airport or establishing designated and restricted uses of various areas of the airport.

“Owner” shall mean a person in whose name the legal title of an aircraft or motor vehicle is held. The lessee or mortgagor of any aircraft or motor vehicle, which is subject to a conditional sale with the right to purchase, and with the immediate right of possession vested in the lessee or one in possession of the aircraft or motor vehicle, shall also be deemed the owner for purposes of these Rules and Regulations.

“Person” shall mean an individual, firm, partnership, corporation, company, association, or joint stock association.

“Propeller Aircraft” shall mean any aircraft powered by reciprocating or turbine engines where majority of thrust is provided by propeller.

“Restricted Area” shall mean any area of the airport, which is locked or has a posted notice, for which access is prohibited or limited to specific authorized persons.

“Rules and Regulations” shall mean these Rules and Regulations, as the same may be amended from time to time.

“Security Background Check” shall mean an investigation into a person’s employment history and a criminal records check conducted pursuant to the procedures set forth in Transportation Security Administration Regulations Section 1500 (or for such successor section as may be currently in force).

“Security Identification Display Area” or **“SIDA”** shall mean those areas of the Airport, if any, designated by the Airport Director, in accordance with Federal Aviation Regulations, in which each individual in the area is required to display on their person the identification badge issued by the Airport Director or such other form of identification approved by the Airport Director.

“Security Program” shall mean that program developed for the airport by the Airport Director, as required and/or approved by the DOT or FDOT, for the protection and safety of aircraft operations and uses of the airport.

“Taxicab” or **“Taxi”** shall mean any automobile that carries persons for a fare, determined by a meter, and that is appropriately licensed as a taxicab by the proper governmental authority.

“Tenant” shall mean a person who leases real property on the airport or from the city (county) for airport-related functions and whose premises have access to the airport. For purposes of these rules, “tenant” shall include sub-tenants and other persons who occupy a tenant’s premises with the consent of the tenant.

“Terminal” shall mean any airport facilities accessed by the public related to air transportation, including all roadways, vehicular circulation areas and parking facilities accessed by the public related to air transportation, including all roadways, vehicular circulation areas and parking facilities associated therewith and including facilities operated by Tenants.

“TODA” shall mean takeoff distance available, as such term is used in Advisory Circular 150/5300-13 as may be amended and/or any other such official document published by FAA.

“TORA” shall mean takeoff run available, as such term is used in Advisory Circular 150/5300-13 as may be amended and/or any other such official document published by FAA.

“TSA” shall mean the Department of Homeland Security’s Transportation Security Administration.

“Vehicle” shall mean anything other than an airport or emergency vehicle, used as a method of transportation for persons and/or goods.

“Zero Tolerance” shall mean that no warning notices, verbal or written, will be issued for violations that have a Zero Tolerance policy. Offenders will immediately be penalized as outlined in these Rules and Regulations.

✈ ✈ ✈

Section IV: Administration

1. Airport Operator: _____
2. Individual responsible for airport security: _____
3. (List the responsibilities of this individual).

For example:

- a. Timely provision of evidence of security measure compliance as may be requested*
- b. Maintaining a complete and current list of all individuals with airport access*
- c. Maintaining documentation of all training provided in accordance with any current Airport Security Procedures*
- d. Maintaining and updating the Airport Security Procedures to reflect the current state of conditions at the airport*
- e. Timely distribution of the Airport Security Procedures or specific parts thereof, to appropriate persons or entities*
- f. Proper dissemination of all correspondence or other communications with airport tenants and others on security related matters*
- g. Daily oversight of security provisions at the airport and ensuring compliance with the Security Procedures*
- h. Other*

Section V: Aircraft Movement Area/Security Control

1. Aircraft Movement Area

Describe an area that may be used for landing, take-off, and surface maneuvering of aircraft including all intermediate unpaved sections of the airfield encompassed on the airport property. You should also include a map or diagram as an attachment.

2. Perimeter Barriers

Describe any perimeter barriers or access controls, such as:

- (a) Fencing*
- (b) Gates*
- (c) Access Control System*
- (d) Airport Locks*
- (e) Key Control System*
- (f) Other*

Section VI: Airport Security Procedures

Describe any Airport Security Procedures, such as:

- (a) Aircraft Security Requirements*
- (b) Pedestrian/Vehicle Access*
- (c) Challenge Procedures*
- (d) Reporting of Suspicious Behavior*
- (e) Other*

Section VII: Airport Emergency Grid Map

Airport operators should consider creating an emergency locator map to be provided to emergency response personnel (fire, EMS, etc.) and law enforcement, as well as airport personnel. The map should identify all relevant areas of the airport on a grid map, such as:

- (a) Runways*
- (b) Ramp Areas*
- (c) Fence Lines*
- (d) Gates*
- (e) Automobile Parking Areas*
- (f) Hydrants*
- (g) Emergency Shelters*
- (h) Buildings*
- (i) Hazardous Materials Sites*
- (j) Other*

Section VIII: Identification of Airport Personnel

Describe any personnel identification methods/systems and the procedures for those that are currently in use, such as:

- (a) Airport-issued identification badge(s) or card(s)*
- (b) Identification Badge/Card application procedures*
- (c) Other acceptable forms of identification*
- (d) Accountability of lost/stolen identification badges/cards*
- (e) Temporary airport identification badges/cards*
- (f) Uniforms which display logo or other identifiable markings*
- (g) Other*

Section IX: Identification of Vehicles

Describe what methods/systems are used to identify authorized vehicles in the air operations area (AOA). The following are examples of methods to identify authorized vehicles:

- (a) Special paint schemes or markings*
- (b) Decal in a specified location on the vehicle*
- (c) Hang tags*

Section X: Law Enforcement

Describe any agreement(s) and responsibilities that the airport owner/operator may have with law enforcement agencies to provide support, traffic control, police patrols, and any emergency responses. Include any written agreements as attachments to the manual.

Section XI: Special Events

Describe any procedures that exist for special events such as:

- (a) Air Shows*
- (b) VIP Visits*
- (c) Events that result in unusual numbers of people on the airport*

Section XII: Increased Security Threats

Describe how security measures are implemented in accordance with the raising and lowering of the Homeland Security Advisory System.

Section XIII: Aviation Security Contingency Plans

Identify and describe all contingency plans and procedures established for security incidents, such as:

- (a) Bomb Threats*
- (b) Civil Disturbances & Crowd Control*
- (c) Air Piracy (Hijacking) Actual or Attempted*
- (d) Suspicious/Unidentified Items*

Section XIV: Model Forms

The following forms have been prepared by the Technical Committee as models that each airport may use or alter to suit the specific needs of their facility. These forms will be posted on www.floridaairports.org for your use. As TSA provides additional recommendations in the future, other forms may be added to the webpage.

- Airport Employee Identification Form
- Transient Aircraft Log
- Contact List
- Access Badge/Vehicle Permit Application
- Criminal History Questionnaire

TRANSIENT AIRCRAFT LOG

Date: _____

Registration Number	Make and Model	ARRIVAL Time	ARRIVING From (if known)	DEPARTURE Time	DEPARTING To (if known)	Contact Name	Phone Number
1							
2							
3							
4							
5							
6							
7							
8							
9							
10							
11							
12							
13							
14							
15							
16							
17							
18							
19							
20							

CONTACT LIST

DATE: _____

EMERGENCY AGENCIES: (Please Print)

Police:

	Name	Phone #
Local:	_____	_____
State:	_____	_____
County:	_____	_____
USFWS:	_____	_____
DOT:	_____	_____
_____	_____	_____
_____	_____	_____

Medical:

	Name	Phone #
Fire/Rescue:	_____	_____
Hospital:	_____	_____
Hospital:	_____	_____
Hospital:	_____	_____
Psychiatric:	_____	_____
_____	_____	_____
_____	_____	_____

Emergency Management:

	Name	Phone #
Local:	_____	_____
County:	_____	_____
State:	_____	_____
HAZMAT:	_____	_____
Health Dept:	_____	_____
_____	_____	_____
_____	_____	_____
_____	_____	_____

AIRPORT ADMINISTRATION (Please Print)

Airport Manager:

Emergency Phone:

Office Phone:

Home Phone:

Other (pagers, personal cell, etc.):

Security Coordinator:

Emergency Phone:

Office Phone:

Home Phone:

Other (pagers, personal cell, etc.):

Operations Manager:

Emergency Phone:

Office Phone:

Home Phone:

Other (pagers, personal cell, etc.):

Other:

Emergency Phone:

Office Phone:

Home Phone:

Other (pagers, personal cell, etc.):

AIRPORT TENANTS (Please Print)

Company: _____

Address: _____

Contact: _____

Title: _____

Emergency Phone: _____

Office Phone: _____

Home Phone: _____

Other (pagers, personal cell, etc.): _____

Company: _____

Address: _____

Contact: _____

Title: _____

Emergency Phone: _____

Office Phone: _____

Home Phone: _____

Other (pagers, personal cell, etc.): _____

Company: _____

Address: _____

Contact: _____

Title: _____

Emergency Phone: _____

Office Phone: _____

Home Phone: _____

Other (pagers, personal cell, etc.): _____

OTHER CONTACTS: (Please Print)

Utility Companies:

	Name	Phone #
Electric:	_____	_____
Phone:	_____	_____
Gas:	_____	_____
Water:	_____	_____
Sewer:	_____	_____
Waste:	_____	_____
Other:	_____	_____
_____	_____	_____
_____	_____	_____

Other Agencies:

	Name	Phone #
FDOT:	_____	_____
FAA:	_____	_____
TSA:	_____	_____
FBI:	_____	_____
DHS:	_____	_____
Customs:	_____	_____
Immigration:	_____	_____
Agriculture:	_____	_____

Surrounding Governments/Departments:

	Name	Phone #
_____	_____	_____
_____	_____	_____
_____	_____	_____
_____	_____	_____
_____	_____	_____

AUTHORIZING AGENT SECTION: (Please Print)

Please have the correct Authorizing Agent sign in the appropriate box for each gate you require access to. **NOTE** Gate Access will be only be given based upon your necessary access level. **For Restricted Movement Area Access, under gate # write "RMA", leave gate location blank.**

Gate #	Gate Location	Authorized Signature	Printed Name/ Location	Personal Vehicle Access Required? <input type="checkbox"/> No <input type="checkbox"/> Yes
				<input type="checkbox"/> No <input type="checkbox"/> Yes
				<input type="checkbox"/> No <input type="checkbox"/> Yes
				<input type="checkbox"/> No <input type="checkbox"/> Yes
				<input type="checkbox"/> No <input type="checkbox"/> Yes

AIRCRAFT INFORMATION SECTION: (Please Print)

	Aircraft 1	Aircraft 2	Aircraft 3
Aircraft N #			
Make			
Model			
Location			
Insurance Company			
Ins. Expiration Date			
Ins. Phone No.			

CONTRACTOR SECTION: (Please Print) CONTRACTORS ONLY

Sponsoring Tenant: _____ Est. Completion Date: _____

Brief Description of Project or Activity: _____

EMPLOYER SECTION (FILLED BY EMPLOYER): REQUIRED ONLY FOR APPLICANTS OBTAINING AN ACCESS CONTROL BADGE THROUGH THEIR EMPLOYEE

Employer/Company Name: _____ Phone: _____

Applicant's Title/Position: _____

I request that the employee identified above be granted an Access Badge for work at the Airport. I agree with the conditions for the privilege stated above. I acknowledge that, as the employer, I am responsible for my employees' entire adherence to the Access Control Procedures, and the Airport Rules and Regulations.

Authorizing Signature: _____ Date: _____

Printed Name: _____ Title: _____

EMPLOYEE SIGNATURE (SIGNED BY APPLICANT): REQUIRED ONLY FOR APPLICANTS OBTAINING AN ACCESS CONTROL BADGE THROUGH THEIR EMPLOYER

In consideration of the Airport granting me an Access Badge, my employer and I agree to, and acknowledge our understanding of the Airports Rules and Regulations and the Airport's Access Control Procedures. My employer has copies of these available for review and I also may review them at the Airport Administration Office, upon request.

A violation of these Rules and Regulations or of the Access Control Procedures may result in penalties.

Applicant Signature: _____ Date: _____

AIRPORT TERMS AND CONDITIONS SECTION

- I agree to return the badge issued by the Airport when use of the badge is no longer required for the purpose for which it was issued or the use is no longer permitted by Airport Management; or when I am no longer employed with the above company; or when the badge is lost or stolen and later recovered; or when the badge has expired.
- I agree to pay all fees, penalties or charges set forth by the Airport for the badge and permits issued to me when these items are no longer required for the purpose for which they were issued; or their use is no longer permitted by the Airport Management; or when I am no longer employed with the above company; or when any of these items are lost or stolen; or have expired and have not been returned to Airport Management, as applicable.
- As a condition of being issued a badge and/or permit, I hereby agree to comply with any policies, provisions, or procedures which the FAA and/or Airport Management have promulgated or promulgate in the future and deem necessary to ensure the security and / or safety of operations at the Airport.
- I understand that failure to comply with any such policies, provisions, or procedures shall be grounds for the immediate revocation of my badge and permit(s) and any privileges conveyed therewith.

APPLICANT SIGNATURE (Required)

I have received from the Airport, an access badge and/or vehicle permit(s). I have read, understand, and will comply with the above statements and all other rules and regulations. I hereby certify there are no misrepresentations, omissions, or falsifications in the information I have provided. Misrepresentations, omissions, falsifications, or violation of any rule/regulation of the Airport is grounds for immediate revocation of the badge/vehicle permit(s).

Applicant Signature: _____ Date: _____

AIRPORT OPERATIONS USE ONLY

Badge #: _____ Date Issued: _____ Issued By: _____

Badge Fees Paid: Yes No Number of Vehicle Permits Received: _____

Vehicle Permit Numbers: _____

Date Applicant Completed Test: _____ Administered By: _____

Movement Area: _____ Non-Movement Area: _____

Data Entered by: _____ Date Terminated Badge Received: _____

Badge Deactivated by: _____

CRIMINAL HISTORY QUESTIONNAIRE

If you answer **YES** to any of the following questions, list question number and details in the space provided below.

1. Yes No Have you ever been arrested, received a notice to appear, charged, convicted, pled nolo contendere, or pled guilty in any jurisdiction to any of the crimes listed below, regardless if the record was sealed or expunged?

- | | |
|---|---|
| (1) Forgery of certificates, false marking of aircraft, and other aircraft registration violation; 49 U.S.C. 46306. | (18) Treason. |
| (2) Interference with air navigation; 49 U.S.C. 46308. | (19) Rape or aggravated sexual abuse. |
| (3) Improper transportation of a hazardous material; 49 U.S.C. 46312. | (20) Unlawful possession, use, sale, distribution, or manufacture of an explosive or weapon. |
| (4) Aircraft piracy; 49 U.S.C. 46502. | (21) Extortion. |
| (5) Interference with flight crew members or flight attendants; 49 U.S.C. 46504. | (22) Armed or felony unarmed robbery. |
| (6) Commission of certain crimes aboard aircraft in flight; 49 U.S.C. 46506. | (23) Distribution of, or intent to distribute, a controlled substance. |
| (7) Carrying a weapon or explosive aboard aircraft; 49 U.S.C. 46505. | (24) Felony arson. |
| (8) Conveying false information and threats; 49 U.S.C. 46507. | (25) Felony involving a threat. |
| (9) Aircraft piracy outside the special aircraft jurisdiction of the United States; 49 U.S.C. 46502(b). | (26) Felony involving—
(i) Willful destruction of property;
(ii) Importation or manufacture of a controlled substance;
(iii) Burglary;
(iv) Theft;
(v) Dishonesty, fraud, or misrepresentation;
(vi) Possession or distribution of stolen property;
(vii) Aggravated assault;
(viii) Bribery; or
(ix) Illegal possession of a controlled substance punishable by a maximum term of imprisonment of more than 1 year. |
| (10) Lighting violations involving transporting controlled substances; 49 U.S.C. 46315. | |
| (11) 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. | |
| (12) Destruction of an aircraft or aircraft facility; 18 U.S.C. 32. | |
| (13) Murder. | |
| (14) Assault with intent to murder. | |
| (15) Espionage. | (27) Violence at international airports; 18 U.S.C. 37. |
| (16) Sedition. | |
| (17) Kidnapping or hostage taking. | (28) Conspiracy or attempt to commit any of the criminal acts listed in this paragraph (d). |

APPENDIX A

Security Guidelines for General Aviation Airports



Transportation Security Administration

Security Guidelines for General Aviation Airports

Information Publication A-001
May 2004

This guidance document was developed by TSA, in cooperation with the General Aviation (GA) community. It is intended to provide GA airport owners, operators, and users with guidelines and recommendations that address aviation security concepts, technology, and enhancements.

The recommendations contained in this document have been developed in close coordination with a Working Group comprised of individuals representing the entire spectrum of the GA industry. This material should be considered a living document which will be updated and modified as new security enhancements are developed and as input from the industry is received. To facilitate this, TSA has established a mailbox to collect feedback from interested parties. Persons wishing to provide input should send Email to General.Aviation@dhs.gov and insert **"GA Airport Security"** in the subject line.

Executive Summary.....	iii
1. Background	1
1.1. The GA Industry	2
1.2. The Aviation Security Advisory Committee (ASAC)	3
1.3. GA Airport Vulnerability	4
2. Airport Characteristics	5
3. Recommendations	8
3.1. Personnel	8
3.1.1. Passengers/Visitors	8
3.1.2. Flight Schools and Student Pilots	9
3.1.3. Aircraft Renters	9
3.1.4. Transient Pilots	10
3.2. Aircraft.....	10
3.3. Airports/Facilities.....	11
3.3.1. Hangars	11
3.3.2. Locks.....	11
3.3.3. Perimeter Control	11
3.3.4. Lighting	12
3.3.5. Signs	12
3.3.6. Identification System.....	13
3.3.7. Airport Planning	14
3.4. Surveillance.....	14
3.4.1. Airport Community Watch Program	14
3.4.2. Reporting Procedures	15
3.4.3. Airport Security Committee	16
3.4.4. Law Enforcement Officer (LEO) Support.....	16
3.4.5. Closed Circuit Television (CCTV)	16
3.4.6. Intrusion Detection Systems (IDS).....	17
3.5. Security Procedures & Communications.....	17
3.5.1. Security Procedures.....	17
3.5.2. Threat Level Increases.....	17
3.5.3. Threat Communication System.....	18
3.6. Specialty Operations	19
3.6.1. Agricultural Aircraft Operations	19
3.6.2. Airport Tenant Facilities	20
3.6.3. Aircraft and Vehicle Fueling Facilities	20
3.6.4. Military Facilities.....	20
Appendix A – Airport Characteristics Measurement Tool	21
Appendix B – Suggested Airport Security Enhancements.....	22
Appendix C – Locks.....	23
Appendix D – Fencing	25
Appendix E – Access Points.....	28
Appendix F – Lighting.....	30
Appendix G – Security Procedures Template.....	31
Appendix H - Bibliography	39
FAA Advisory Circulars	39

U.S. Government Regulations 40
Other Reports 40
Appendix I – Useful Websites..... 42
Aviation Trade Associations..... 42
Federal Government..... 42
Other References..... 42

Executive Summary

The purpose of the Security Guidelines for General Aviation Airports Information Publication (IP) is to provide owners, operators, sponsors, and other entities charged with oversight of GA airports a set of federally endorsed security enhancements and a method for determining when and where these enhancements may be appropriate. The document does not contain regulatory language nor is it intended to suggest that any recommendations or guidelines should be considered a mandatory requirement. However, program requirements for operators regulated under the Twelve-Five and Private Charter Rules are not addressed in this document, remain in effect, and may be incorporated into airport security procedures if appropriate.

TSA launched this project, working collaboratively with key stakeholders, to develop and disseminate appropriate security guidelines for general aviation airports and heliports. A Working Group was established under the Aviation Security Advisory Committee (ASAC) to compile a list of recommended security best practices used throughout the industry. The ASAC delivered its recommendations to TSA in November 2003. These recommendations form the framework for the IP and all of the ASAC recommendations were incorporated.

The document offers an extensive list of options, ideas, and suggestions for the airport operator, sponsor, tenant and/or user to choose from when considering security enhancements for GA facilities. This guidance will provide consistency across the Nation with regard to security at GA facilities.

The IP also provides a method to discriminate security needs at differing airports. The Airport Characteristics Measurement Tool is a self administered method by which an airport operator can assess an airport's security characteristics and decide which security enhancements would be most appropriate in that particular environment.

The IP outlines seven functional areas of GA airport security. The functional areas include:

- Personnel
- Aircraft
- Airports/Facilities
- Surveillance
- Security Plans and Communications
- Specialty Operations

Each of the functional areas is further broken down into detailed discussions of methods and strategies for enhancing general aviation security.

This is a living document, that is initially being released as Version 1.0 and which will continue to be refined with input from stakeholders.

1. Background

The purpose of this Information Publication is to provide owners, operators, sponsors, and other entities charged with oversight of GA landing facilities with a set of security best practices and a method for determining when and where these enhancements would be appropriate. Regarding GA, a few definitions are in order:

- GA, as used in this document, means all civil aviation except for scheduled passenger and scheduled cargo service and military aviation.
- Airports, as used in this document, means an area of land or water that is used or intended to be used for the landing and takeoff of aircraft, and includes its buildings and facilities, if any. However, this document does not apply to airports required to comply with the provisions of 49 CFR 1542 or military airports.

This document does not contain regulatory language. It is not intended to suggest that any recommendations or guidelines contained herein might be considered as mandatory requirements to be imposed upon GA facilities or operators, nor are these recommendations and guidelines intended to suggest any specific or general criteria to be met in order to qualify for Federal funding. The intent of this document is to provide a tool that enables GA landing facility managers to assess vulnerabilities and tailor appropriate security measures to their environment – not to 'stigmatize' airports in any way.

Recognizing that every GA landing facility is unique, there are recommendations and guidelines contained in this document that might be considered highly beneficial in one airport environment while being virtually impossible to implement at another facility. The purpose of the document is to provide an extensive list of options, ideas, and suggestions for the airport operator, sponsor, tenant and/or user to choose from when considering security enhancements for GA facilities. When stating in this document that a measure "should" be used it means the measure is recommended to the extent it is consistent with the airport's circumstances as discussed throughout this document. The Transportation Security Administration (TSA) intends that this document be used to provide effective and reasonable security enhancements at GA facilities across the Nation.

To date there have been numerous initiatives undertaken by the GA industry to develop GA airport security guidelines such as awareness programs, reporting methods, and educational courses. These efforts have been considered by TSA and are reflected in this guidance document.

Please note that throughout this document many airport terms are used that are the same as or similar to those terms used when describing airports required to comply with the security regulations outlined in 49 CFR Part 1542. It is not the intent of this document to recommend that GA landing facilities meet the same

security requirements as commercial service airports. However, on occasion it is necessary to use terminology that airport operators are already familiar with in order to facilitate readers' understanding. Additionally, references are made to Federal Aviation Administration (FAA) guidance materials normally related to commercial service airports and operations. These documents are provided as reference material but may not necessarily constitute an appropriate approach to GA security at your facility.

1.1. The GA Industry

As previously stated, as used in this document, GA encompasses all civil aviation, except military aviation and passenger and scheduled cargo service. Some basic statistics available regarding the industry:

- More than 19,000 landing facilities nationwide, including heliports, lakes, and dirt landing strips in remote wilderness areas as well as GA airports near urban settings that rival the size and scope of some air carrier airports.
- More than 200,000 GA aircraft in the U.S. are responsible for 75% of all air traffic.
- FAA certificated and non-certificated aircraft range from one-person ultralights and powered parachutes with extremely limited range and payload capabilities to helicopters, seaplanes, vintage, fabric-and-wood biplanes, experimental airplanes, four-seat single-engine airplanes, twin turboprops, and large and small business jets.
- GA accounts for over 1.3 million jobs, with nearly \$20 billion in annual earnings. Its direct and indirect economic impact exceeds \$102 billion annually.
- There are more than 630,000 certificated pilots in the U.S., most of whom conduct GA flight operations.
- GA transports approximately 145 million passengers annually in aircraft of all sizes for business and personal reasons.
- An estimated 58% of all GA flights are conducted for business and corporate travel.
- Commercial, non-scheduled flights (charters) are also a component of GA, with more than 22,000 pilots flying some 14,700 aircraft for this industry segment during 2001 alone.
- GA aircraft are used for a wide range of flight operations including personal/family transportation, training, MEDEVAC, transporting medical supplies, emergency services, rescue operations, wildlife surveys, traffic reporting, agricultural aviation, firefighting, and law enforcement.

(Sources: December 2003 FAA Administrator's Fact Book; GA Serving America www.gaservingamerica.com; National Air Transportation Association)

Because of the wide variety and scope of GA aircraft and landing locations, any approach to implementing security guidelines must consider the various types of flight operations as well as the size of aircraft involved, among other factors. Therefore, a flexible, common-sense approach to GA airport security is important if the industry is to retain its economic vitality.

1.2. *The Aviation Security Advisory Committee (ASAC)*

Following the 1988 Pan American World Airways Flight 103 tragedy, it was determined a need existed for all segments of the aviation industry to have input into future aviation security considerations. In response, the Aviation Security Advisory Committee (ASAC) was established in 1989 and was managed by the Federal Aviation Administration (FAA). After the terrorist attacks of September 11, 2001, Congress enacted the Aviation and Transportation Security Act (ATSA), which created the TSA. Congress established TSA to develop, regulate, and enforce transportation security standards for all modes of transportation. Consistent with this mission, Congress transferred the bulk of FAA's civil aviation security responsibilities to TSA. Accordingly, sponsorship of the ASAC was also transferred to TSA.

In April 2003, TSA requested ASAC to establish a working group made up of industry stakeholders to develop guidelines for security enhancements at the nation's private and public use GA landing facilities. TSA made this request because, in the absence of a unified set of federal security standards for GA airports, some state and local governments had begun developing their own airport-related security requirements. TSA recognized that this could result in varied state and local security requirements that could pose an unnecessary burden on airport owners and operators while leaving security gaps in other locations. TSA believed that a better approach would be to address GA airports (both public and private use) in a collaborative forum in order to develop a set of industry endorsed guidelines and "best practices" that are tailored to broad categories of airports.

The Working Group represented the GA industry as a whole. Participating members included:

- Aircraft Owners & Pilots Association (AOPA)
- Airport Consultants Council (ACC)
- American Association of Airport Executives (AAAE)
- Experimental Aircraft Association (EAA)
- GA Manufacturers Association (GAMA)
- Helicopter Association International (HAI)
- National Air Transportation Association (NATA)
- National Association of State Aviation Officials (NASAO)
- National Business Aviation Association (NBAA)
- United States Parachute Association (USPA)

Additionally, GA airport managers and representatives of various state government aviation agencies fully participated in the working group's activities.

1.3. GA Airport Vulnerability

Historically, GA airports have not been subject to federal rules regarding airport security. Prior to September 11, 2001, the federal government's role in airport security focused exclusively on those airports serving scheduled operations. Now, however, TSA must examine all aspects of the transportation system for vulnerabilities to terrorist activities. To date TSA has not required GA airports to implement security measures except for those facilities located within the Washington DC Airspace Defense Identification Zone Flight Restricted Zone. Nevertheless, many GA airport managers commonly implement basic security measures found throughout the nation's airports. Examples include fencing and access control devices for vehicle and pedestrian gates, daily airfield inspections, landside and airfield signage, and public awareness programs for educating the aviation community as well as the general public on the safe and secure use of the facility.

TSA has not taken a position that GA airports and aircraft are a threat, in and of themselves. However, as vulnerabilities within other areas of aviation have been reduced, GA may be perceived as a more attractive target and consequently more vulnerable to misuse by terrorists. TSA believes that the security guidelines outlined in this document will help airport managers and aircraft operators determine which security measures they should take at their particular facility to reduce vulnerabilities and encourage the adoption of consistent and appropriate security measures across the nation. TSA also believes that these security guidelines must be federally endorsed to discourage a hodgepodge of state and local guidelines.

By definition the term GA includes a broad range of aircraft and aviation activity. Not surprisingly, GA airports vary greatly in size, function and operational characteristics. Just as all commercial service airports differ in their security needs the same is true with GA airports. TSA understands that one size security will not fit the entire spectrum of GA airports. For example, a privately owned landing strip in a rural area would not need to implement the same security measures as a large corporate GA airport near a major metropolitan area. While the potential for misuse of an aircraft operating from the rural airport exists, required adherence to a single requirement across the nation is physically and economically impossible and clearly not reasonable. TSA must instead focus on managing the risk associated with GA facilities recognizing the characteristics that define each facility.

The ability (physically and financially) of GA airports to voluntarily implement security improvements varies greatly. The majority of these facilities are not self-sustaining in the same manner as commercial service airports. Consequently, the decision to implement security measures must include consideration of economic feasibility and reasonableness.

2. Airport Characteristics

Airport Characteristics Measurement Tool

In order to assess which security enhancements are most appropriate for a GA landing facility, consideration must be given to those elements that make the airport unique. The most appropriate party to do this would be the person or persons with day-to-day operational control over the facility. This could be a state official, airport manager, or fixed base operator (FBO). In any case, the party doing the assessment should be intimately familiar with the airport, its activities, and the surrounding areas.

To assist in this effort, TSA has developed an Airport Characteristics Measurement Tool (found in Appendix A) that can be used to determine where in the risk spectrum the facility lies. The tool is a list of airport characteristics that potentially affect a facility's security posture. Each of the characteristics is assigned a point ranking, the idea being that certain characteristics affect the security at an airport more so than others.

The characteristics have been broken down into the following categories:

- **Airport Location** – A facility's proximity to mass population areas or sensitive sites can affect its security posture. **For the purpose of this guidance we are considering a mass population area to be an area with a total metropolitan population of at least 100,000 people. A sensitive site is defined as an area which would be considered a key asset or critical infrastructure of the United States. Sensitive sites can include certain military installations, nuclear and chemical plants, centers of government, monuments and iconic structures, and/or international ports.** Distance from such sites directly affects the ability of responding agencies to effectively react to an event. The further away from a potential target, the greater the response time available to responding agencies.
- **Based Aircraft** – A smaller number of based aircraft increases the likelihood that illegal activities would be identified more quickly than at airports with a large number of based aircraft. In addition, airports with based aircraft of over 12,500 pounds warrant greater scrutiny.

- **Runways** – Airports with longer paved runways are able to serve larger aircraft and consequently should be more security conscious. Conversely, because shorter, unpaved runways are not practical for use by large aircraft in many weather conditions, they may present a less attractive launching point for terrorist activities. **Airport operators at facilities with multiple runways should only consider the longest operational runway on the airport.**

Please note: TSA recognizes that airports at higher elevations may need longer runways to accommodate even the smallest of aircraft. It is not the intent of this document to assess points for a longer runway if it is unrealistic that the runway could be used for larger aircraft operations. Individuals using the Airport Characteristics Measurement Tool should understand that the baseline of the Tool was developed to consider aircraft performance at approximately sea level.

- **Operations** – The number and types of operations that are conducted at an airport call for different approaches to security. **Consider all operations including those operations that are only infrequently conducted at your airport.**

Additionally, there is a distinct difference between “public use” airports and “private use” airports. Privately-owned, private-use GA airports receive no public funds and most state government aviation agencies currently have no authority to regulate them. However, TSA believes that some of the guidelines in this report would be beneficial to enhancing the security at these facilities as well.

To use the tool, you should choose those characteristics that apply to your facility. Each of the characteristics is assigned a point value from 0-5 as shown in the Appendix A Tool. Assess points for **every** characteristic that applies to your facility (except for runway length considerations, there may be more than one selection in each category) and total the number of points scored.

Example 1

Security Characteristics	Public Use Airport/Heliport
Small, rural, public use field located a significant distance from any sensitive sites	0
15 based aircraft	1
2500' runway	4
Asphalt runway	1
Flight training is conducted on airfield	3
Total	9

Example 2

Security Characteristics	Public Use Airport/Heliport
Airport within 30nm of a sensitive site	4
Within the boundaries of Class B airspace	3
50 based aircraft	2
5000' runway	5
Asphalt runway	1
More than 50,000 aircraft operations per year	4
Part 135 operations	3
Flight training is conducted on airfield	3
Rental aircraft	4
Total	29

Suggested Airport Security Enhancements

Appendix B contains groupings of security enhancements that may be appropriate for those facilities scoring within a certain point range on the Airport Characteristics Measurement Tool. The lists of suggested security enhancements are grouped according to the point range totals derived using the Measurement Tool. These lists are by no means complete for every facility, nor are they the only method for improving security. They are suggestions that could be useful at these locations. They should not be used as the sole means of determining what security precautions are appropriate. Instead, airport owners and operators should rely on their experience and intimate knowledge of their facility, applying those items that are both reasonable and effective.

This list is an assessment of the most significant characteristics relating to GA airport security. The scope and breadth of GA landing facilities precludes any one document from capturing all characteristics relevant to all GA airports. Users are advised to consider all characteristics germane to security at their particular facility when using the Airport Characteristics Measurement Tool.

Mitigating Characteristics

TSA also recognizes that some characteristics of GA airports actually serve the purpose of enhancing security, such as having a police presence on the airport property. Other characteristics may negate the need for certain security measures, such as if all of an airport's runways are grass. Airport operators should use their best judgment when considering mitigating characteristics and their effect on which security enhancements are to be implemented at their airport. Some examples of mitigating circumstances are:

- Operating air traffic control tower on the field
- 24/7 airport staffing
- Federal, state, local, or contract law enforcement on airport property
- All based aircraft under 1500 lbs

- All runways are grass
- Restricted access to the airport
- Require ID badges
- Documented security Procedures

3. Recommendations

Managers and operators of GA airports are encouraged to use the recommended guidelines in this report to enhance the security of their respective facilities. Intrinsic in these recommended guidelines is the concept that GA airports are extremely diverse and that appropriate security measures can be determined only after careful examination of an individual airport. The key findings of the report are encompassed in the following areas:

- Personnel
- Aircraft
- Airports and Facilities
- Surveillance
- Security Procedures and Communications
- Specialty Operations

3.1. *Personnel*

3.1.1. Passengers/Visitors

A key point to remember regarding GA passengers is that the persons on board these flights are generally better known to airport personnel and aircraft operators than the typical passenger on a commercial airliner. Recreational GA passengers are typically friends, family, or acquaintances of the pilot in command. Charter/sightseeing passengers typically will meet with the pilot or other flight department personnel well in advance of any flights. Suspicious activities such as use of cash for flights or probing or inappropriate questions are more likely to be quickly noted and authorities could be alerted. For corporate operations, typically all parties onboard the aircraft are known to the pilots. Airport operators should develop methods by which individuals visiting the airport can be escorted into and out of aircraft movement and parking areas. By utilizing common sense suggestions, the GA community can help ensure the security of their airport. Prior to boarding, the pilot in command should ensure that:

- The identity of all occupants is verified,
- All occupants are aboard at the invitation of the owner/operator, and
- All baggage and cargo is known to the occupants.

3.1.2. Flight Schools and Student Pilots

We now know that the September 11 terrorists trained at flight schools in Florida, Arizona, and Minnesota. This has raised concerns among the public and federal law enforcement organizations about flight school security and how it can be improved.

In response the federal government and the aviation industry have developed the following recommendations designed to enhance positive control of the aircraft before movement, when an instructor is ready to accompany the student. Flight schools should:

- Require flight students to use proper entrances and exits to ramp areas. If access controls are available, consider having flight school personnel allow access to ramp areas only after establishing positive identification of flight students.
- Establish positive identification of student pilots prior to every flight lesson.
- Control aircraft ignition keys so that the student cannot start the aircraft until the instructor is ready for the flight to begin.
- Limit student pilot access to aircraft keys until the student pilot has reached an appropriate point in the training curriculum.
- Consider having any student pilot check in with a specific employee (i.e. dispatcher, aircraft scheduler, flight instructor, or other "management" official) before being allowed access to parked aircraft.
- Have the student sign or initial a form and not receive keys until an instructor or other "management official" also signs or initials.
- When available, use a different ignition key from the door lock key. The instructor would provide the ignition key when he or she arrives at the aircraft.

TSA is developing a security awareness training program for use by flight schools that may also be used by GA airports. The training program will provide information on suspicious behavior patterns, appropriate responses to such behavior, and GA airport watch programs. The training program will be available electronically on the TSA GA website (www.tsa.gov/public/display?theme=180) in the summer of 2004. The GA website also will contain information regarding any general threats to GA airports or aircraft and major incidents involving GA airports or aircraft.

3.1.3. Aircraft Renters

A very large proportion of GA aircraft are used for rental purposes. At most airports, regular aircraft renters are fairly well known, and new renters are typically required by insurance agencies to complete a flight check which ascertains their ability to safely operate rental aircraft. Both of these factors may serve as a deterrent to using GA aircraft for terrorist purposes. However, developing and documenting standard procedures and ensuring flight school

employees are educated in the procedures further enhances flight school security.

- The identity of an individual renting an aircraft should be verified by checking an individual's government-issued photo ID as well as his or her airman certificate and current medical certificate necessary for that operation.
- In addition to any aircraft-specific operational and training requirements, a first-time rental customer should be familiarized with local airport operations, including security procedures used at the facility.
- Operators providing rental aircraft should be vigilant for suspicious activities and report them to appropriate officials.

3.1.4. Transient Pilots

Airport personnel should strive to establish procedures to identify non-based pilots and aircraft using their facilities. One helpful method would be for airport or FBO operators to establish sign-in/sign-out procedures for all transient operators and associate them with their parked aircraft. Having assigned spots for transient parking areas can help to easily identify transient aircraft on an apron.

3.2. Aircraft

The main goal of enhancing GA airport security is to prevent the intentional misuse of GA aircraft for terrorist purposes. Proper securing of aircraft is the most basic method of enhancing GA airport security. Pilots should employ multiple methods of securing their aircraft to make it as difficult as possible for an unauthorized person to gain access to it.

Some basic methods of securing a GA aircraft include:

- Ensuring that door locks are consistently used to prevent unauthorized access or tampering with the aircraft.
- Using keyed ignitions where appropriate.
- Storing the aircraft in a hangar, if available, and locking hangar doors.
- Using an auxiliary lock to further protect aircraft from unauthorized use. Commercially available options for auxiliary locks include locks for propellers, throttle, and tie-downs.
- Ensuring that aircraft ignition keys are not stored inside the aircraft.

3.3. Airports/Facilities

3.3.1. Hangars

Storage in hangars is one of the most effective methods of securing GA aircraft. TSA recognizes that hangar space at many airports is limited. However, every attempt should be made to utilize hangars when available and ensure that all hangar/personnel doors are secured when unattended.

Hangars should be properly marked and numbered for ease of emergency response. These areas are also a good place to install security and informational signs. Hangar locks that have keys that are easily obtained or duplicated should be avoided. Hangar locks should be rekeyed with every new tenant. Proper lighting around hangar areas should be installed. As an additional security measure alarm and intrusion detection systems could also aid in the security of hangars.

3.3.2. Locks

Regardless of its quality or cost a lock is simply a delaying device and not a complete bar to entry. As important as the choice of lock is, the decision where to install locks is more important. Such factors to consider may include:

- Is the object to be locked indoors or outdoors?
- How many people will need to use the lock (i.e. would a combination be better than issuing keys)?
- Would a certain type of lock impede access in high traffic areas?
- How secure should the area be made?
- Is the area monitored?
- How often will codes, keys, or locks need to be changed for persons needing access (e.g. new hangar tenants, those with tiedown agreements needing ramp access, etc.)?
- Will use of a lock interfere with fire code egress requirements?

A more detailed discussion of locks and their use can be found in Appendix C.

3.3.3. Perimeter Control

To delineate and adequately protect security areas from unauthorized access it is important to consider boundary measures such as fencing, walls, or other physical barriers, electronic boundaries (e.g. sensor lines, alarms), and/or natural barriers. Physical barriers can be used to deter and delay the access of unauthorized persons onto sensitive areas of airports. Such structures are usually permanent and are designed to be a visual and psychological deterrent as well as a physical barrier. They also serve to meet safety requirements in many cases. Where possible, security fencing or other physical barriers should be aligned with security area boundaries.

The choice of an appropriate security boundary design is not only affected by the cost of equipment, installation, and maintenance, but also by effectiveness and functionality, that is, its ability to prevent unauthorized access.

However, it is important to note that perimeter control methods alone will not necessarily prevent a determined intruder from entering, nor may they be appropriate for every facility. The strength of any security mechanism is dependent on the airport's overall security plan. Expending resources on an unnecessary security enhancement (e.g. complete perimeter fencing, and access controls) instead of a more facility specific, reasonable, and more effective method (e.g. tiedown chains with locks) may actually be detrimental to an airport's overall security posture.

More specific information on perimeter control can be found in Appendices D and E.

3.3.4. Lighting

Protective lighting provides a means of continuing a degree of protection from theft, vandalism, or other illegal activity at night. Security lighting systems should be connected to an emergency power source, if available. Requirements for protective lighting of airports depend upon the local situation and the areas to be protected. A careful analysis of security lighting requirements should be based on the need for good visibility and the following criteria: employee recognition and badge identification, vehicle access, detection of intruders, and deterrent to illegal entry. Protective lighting is generally inexpensive to maintain, and when properly employed, may provide airport personnel with added protection from surprise by a determined intruder. However, when developing any security lighting plan care should be taken to ensure that lighting does not interfere with aircraft operations.

Consider installing outdoor area lighting to help improve the security of aircraft parking and hangar areas, fuel storage areas, airport access points; and other appropriate areas.

A more detailed discussion of lighting can be found in Appendix F.

3.3.5. Signs

The use of signs provides a deterrent by warning of facility boundaries as well notifying of the consequences for violation. Signs along a fence line should be located such that when standing at one sign, the observer is able to see the next sign in both directions. While signs for security purposes should be designed to

draw attention, it also should be coordinated with other airport signs for style and consistency when possible. Signs should be constructed of durable materials, contrasting colors, and reflective material where appropriate. Use as concise language as possible.

Wording may include – but is not limited to – warnings against trespassing, unauthorized use of aircraft and tampering with aircraft, and reporting of suspicious activity. Signage should include phone numbers of the nearest responding law enforcement agency, 9-1-1, or TSA's 1-866-GA-SECUR (see section 3.4.2), whichever is appropriate.

Many locations with access control or Closed Circuit Television (CCTV) equipment may warrant signage for directional, legal, or law enforcement purposes (e.g. "Alarm will sound if opened", "Authorized personnel only", "Notice: All activities in this area are being monitored and recorded", etc.).

For more information refer to Advisory Circular (AC) No: 150/5360-12D, Airport Signing and Graphics. At international airports, designers and airport authorities may also wish to consult the International Civil Aviation Organization (ICAO) Document 9430-C/1080, International Signs to Provide Guidelines to Persons at Airports.

3.3.6. Identification System

Some airport operators may wish to consider implementing a method of identifying airport employees or authorized tenant access to various areas of the airport. Currently, there are many systems on the market that may accomplish this. They can range from a simple laminated identification card that includes a photograph of an individual to a sophisticated swipe card with various biometric data. With any identification system, procedures should be developed that include ensuring control and accountability of the media.

Some elements that could be part of an identification system include:

- A full-face image
- The individual's full name
- Airport name
- Employer
- A unique identification number
- The scope of the individual access and movement privileges (e.g. color coding)
- A clear expiration date

A vehicle identification system may be developed. Such a system can assist airport personnel and law enforcement in identifying authorized vehicles. Vehicles can be identified through use of decals, stickers, or hang tags. Decals

should be nontransferable; that is, they should not be capable of being removed without destroying their integrity. These systems should also be used to indicate access authorization where appropriate, such as by numbering or color-coding. Issuing authorities should also attempt to make current stickers/decals easily distinguished from expired ones. In addition, any decal application form should contain owner contact information that may be used in the event of an emergency.

More suggestions for establishing an identification system can be found in AC-107-1, "Aviation Security – Airports".

3.3.7. Airport Planning

Planning for security should be an integral part of any project undertaken at an airport. The most efficient and cost effective method of instituting security measures into any facility or operation is thorough advance planning and continuous monitoring throughout the project. Selecting, constructing, or modifying a facility without considering the security implications can result in costly modifications and delays. Airport operators should consider addressing future security needs such as access controls and lighting enhancements when planning new hangars or terminal buildings. Security concerns should be included and addressed in airport facility and land leases, airport rules and regulations, and the Minimum Standards document. In addition, airport construction projects can affect airfield security. Construction personnel and vehicle access during projects should be considered.

3.4. Surveillance

3.4.1. Airport Community Watch Program

The vigilance of airport users is one of the most prevalent methods of enhancing security at GA airports. Typically, the user population is familiar with those individuals who have a valid purpose for being on the airport property. Consequently, new faces are quickly noticed. Teaching an airport's users and tenants what to look for with regard to unauthorized and potentially illegal activities is essential to effectively utilizing this resource. Airport managers can either utilize an existing airport watch program or establish their own airport specific plan. A watch program should include elements similar to those listed below. These recommendations are not all-inclusive. Additional measures that are specific to each airport should be added as appropriate, including:

- Coordinate the program with all appropriate stakeholders including airport officials, pilots, businesses and/or other airport users.
- Hold periodic meetings with the airport community.
- Develop and circulate reporting procedures to all who have a regular presence on the airport.

- Encourage proactive participation in aircraft and facility security and heightened awareness measures. This should include encouraging airport and line staff to 'query' unknowns on ramps, near aircraft, etc.
- Post signs promoting the program, warning that the airport is watched. Include appropriate emergency phone numbers on the sign.
- Install a bulletin board for posting security information and meeting notices.
- Provide training to all involved for recognizing suspicious activity and appropriate response tactics. This could include the use of a video or other media for training. The following are some recommended training topics:
 - Aircraft with unusual or unauthorized modifications.
 - Persons loitering for extended periods in the vicinity of parked aircraft, in pilot lounges, or other areas deemed inappropriate.
 - Pilots who appear to be under the control of another person.
 - Persons wishing to rent aircraft without presenting proper credentials or identification.
 - Persons who present apparently valid credentials but who do not display a corresponding level of aviation knowledge.
 - Any pilot who makes threats or statements inconsistent with normal uses of aircraft.
 - Events or circumstances that do not fit the pattern of lawful, normal activity at an airport.
- Utilize local law enforcement for airport security community education.
- Encourage tenants to make their staff aware of the airport watch programs.

3.4.2. Reporting Procedures

It is essential that every airport employee, tenant, and user is familiar with reporting unusual or suspicious circumstances on airport property. There are three basic ways that persons can report suspect activities. First is to airport management. Oftentimes questions regarding the legitimacy of an activity can be quickly and easily resolved by bringing it to the attention of an airport employee.

A second method is to utilize the GA-SECURE Hotline. TSA developed and implemented a GA hotline in partnership with the National Response Center. 866-GA-SECUR (1-866-427-3287) was launched on December 2, 2002 and operates 24 hours per day 7 days per week. The GA Hotline serves as a centralized reporting system for general aviation pilots, airport operators, and maintenance technicians wishing to report suspicious activity at their airfield.

The third and most obvious method is to contact local law enforcement using a local phone number or by dialing 911. In instances where the situation could potentially turn dangerous all pilots are strongly encouraged to use this method. However, after contacting 911 or airport management TSA also requests that callers contact the GA Hotline in order to ensure that information surrounding the incident reaches the National Response Center.

3.4.3. Airport Security Committee

Airport management should consider establishing an Airport Security Committee. This Committee should be composed of airport tenants and users drawn from all segments of the airport community. The main goal of this group is to involve airport stakeholders in developing effective and reasonable security measures and disseminating timely security information. Meetings should be held regularly for the purpose of giving coordinated direction to the overall airport security program.

3.4.4. Law Enforcement Officer (LEO) Support

It is imperative that airport operators establish and maintain a liaison with appropriate law enforcement agencies including local, state, and federal. These organizations can better serve the airport operator when they are familiar with airport operating procedures, facilities, and normal activities. Procedures may be developed to have local LEOs regularly or randomly patrol ramps and aircraft hangar areas, with increased patrols during periods of heightened security.

Airport operators should communicate and educate local law enforcement agencies on operational and security procedures at the airport. This may include:

- Recognizing proper airport credentials (e.g. airport ID badges, airmen certificates).
- Recognizing those airport users authorized to drive on the ramp.
- Notifying LEOs as to how they can obtain airport access (e.g. who has gate keys, access codes).
- Educating LEOs on airport speed limits, aircraft right-of-way procedures, and other "normal" operations.
- Issuing airport maps with a detailed facility index.
- Recognizing "normal" airport operations.

3.4.5. Closed Circuit Television (CCTV)

Although CCTV is used for many purposes, its most common use is for surveillance. CCTV systems make it possible for fewer individuals to maintain a constant watch on all areas of the facility. These systems may even provide an alternative to fencing as a method of perimeter security. In conjunction with a perimeter fence, CCTV may also deter security breaches at airports, and may provide an improved response when breaches do occur. Additionally, CCTV video recorders may provide a visual record that can be used to document

activities that become the subject of investigations. However, the inherent weakness of this system is that it must be monitored to be effective. CCTV may be appropriate only at busier, more complex airports.

3.4.6. Intrusion Detection Systems (IDS)

IDS are becoming more and more popular as a method for providing GA airport security. The inherent benefit to such systems is that they can replace the need for physical security personnel to patrol an entire facility or perimeter. Typically, such systems are constantly monitored by a contracting company. If an intrusion or some other specified event (e.g. fire or power outage) is detected, the system administrator notifies police, fire, and/or airport management. Costs vary depending upon the type of system, monitoring fees, and equipment. Such systems can be used to secure terminals, hangars, or other airport facilities, or be used to monitor perimeter security and access points.

3.5. Security Procedures & Communications

3.5.1. Security Procedures

GA airport managers/operators may find it helpful to develop written security procedures. Many of these security initiatives are already being conducted on airfields but have not been formalized into a documented program. Documentation provides managers with a traceable and auditable method of ensuring airport employees and tenants are aware of and understand security issues. Such a protocol should minimally consist of, but not be limited to, airport and local law enforcement contact information, including alternates when available, and utilization of a program to increase airport user awareness of security precautions such as Airport Watch.

Because security procedures may contain sensitive information, the airport operator should limit access to them to the extent possible.

A procedures template can be found in Appendix G.

3.5.2. Threat Level Increases

The Homeland Security Advisory System (HSAS) is a mechanism for the Department of Homeland Security to disseminate information regarding the risk of terrorist acts throughout the nation. It provides airport operators with information to implement increased security measures during times of heightened alert and to reduce security procedures at lower threat levels.

A written GA security procedure can include reference to and be coordinated with appropriate local response plans as prepared for the specific region in which the landing facility is located. The protocol should emphasize such critical elements as awareness, prevention, preparation, response, and recovery. Intrinsic in

these recommended guidelines is the concept that each GA airport is unique. Airport operators are encouraged to develop response procedures appropriate to their facility. During times of lower alert levels airport operators may wish to do the following:

- Develop preparedness plans, emergency contact lists, and training programs to ensure key elements of HSAS and preparedness plans are presented to all employees.
- Review and update any previously developed preparedness plans, emergency contact lists, and training programs.
- Communicate with appropriate local federal agency representatives (e.g. DHS, FBI, and TSA).
- Conduct surveillance of facility property, buildings, and aircraft.
- Coordinate emergency plans as appropriate with nearby jurisdictions.
- Hold security committee meetings to ensure timely dissemination of security/threat information.

Under most circumstances, the measures for increased alert levels (Orange or Red) are not intended to be sustained for substantial periods. Appropriate actions may include:

- Conducting all measures taken at lower threat condition.
- Limiting facility access points.
- Making regular surveillance patrols of facility property, buildings, and aircraft.
- Increasing surveillance of critical locations.
- Coordinating necessary security efforts with federal, state, and local law enforcement agencies or any National Guard or other appropriate organizations.
- Preparing to execute contingency procedures, as appropriate.
- Ensuring positive identification of pilots and tenants.
- Assigning emergency response personnel, pre-positioning, and mobilize specially trained teams or resources.
- Closing the facility.

3.5.3. Threat Communication System

The development of a comprehensive contact list is recommended to be included in any airport security procedures. The list should be distributed all appropriate individuals. The following phone numbers should be included on the contact list (include after hour contact numbers where appropriate):

- Landing facility operator
- Landing facility manager
- Individual with responsibility for facility security

- Local Police or County Sheriff Department (List all responding LEO Agencies)
- State Aviation Director
- County/City Emergency Manager
- State Police
- Fire Department
- State Office of Public Safety/Homeland Security
- FBI
- Local FAA contact
- Local TSA contact (that is, Federal Security Director or designee)
- Any other appropriate organization

Additionally, in the event of a security incident, it is essential that first responders and airport management have the capability to communicate. Where possible, coordinate radio communication and establish common frequencies and procedures to establish a radio communications network with local law enforcement.

Also important to the communication process is a means by which all new security policies, procedures, and alerts are communicated to tenants and other airport users. One method of accomplishing this is to conduct regular meetings with airport tenants and the flying public to discuss security issues and challenges, establishing a centralized area for posting of security information, or even developing an email alert system.

3.6. Specialty Operations

3.6.1. Agricultural Aircraft Operations

TSA recognizes the proactive steps taken by agricultural aircraft operators to secure the industry. TSA suggests that each owner/operator take appropriate steps to secure agricultural aircraft when unattended, including:

- Use multiple devices to secure agricultural aircraft such as throttle and control locks, propeller locks, and hidden ignition switches.
- Store aircraft in hangars with electronic security systems and steel doors.
- Park heavy equipment in the front and back of agricultural aircraft when hangars are not available for storage.

Additional security measures can be found on the National Agricultural Aircraft Association's website at: <http://www.agaviation.org/>

3.6.2. Airport Tenant Facilities

For those airports with a perimeter fence, many airport tenant facilities have access to the aircraft parking and movement and public areas of the airport through their building. Typically, the tenant leasing the facility is responsible for security. However their access controls may also be incorporated into the airport's security procedures and/or alarm and reporting system. Airport operators should coordinate with their tenants to ensure that any security procedures or systems do not conflict or leave gaps. For example, airport management should coordinate and ensure security procedures exist and are harmonized with maintenance facilities that have access on both the public side of the fence and the aircraft parking and movement areas.

3.6.3. Aircraft and Vehicle Fueling Facilities

Fuel farms are normally placed in as remote a location of the airport as possible for safety and convenience purposes. If feasible, use security fencing, lighting, and access controls whenever possible to control movement in these areas. Trucks used to transfer fuel to aircraft should be secured when not in use. This includes controlling fuel truck keys and not leaving keys in trucks while unattended. Consider marshalling fuel trucks in an easily monitored location.

3.6.4. Military Facilities

Some airports may have adjacent or on-airport military facilities such as military Reserve, National Guard, or active duty units. Since each of these situations is unique, and since these facilities are often at least partly within the aircraft movement area, detailed coordination between the airport and the military facility must occur for security procedures and responses. Typical areas of coordination include access control, badging and background check requirements, areas of access, security patrol boundaries, security response responsibilities, and joint and/or shared security system data and equipment.

Appendix A – Airport Characteristics Measurement Tool

Security Characteristics	Assessment Scale	
	Public Use Airports/Heliports	Private Use Airports/Heliports
Location		
Within 30 nm of mass population areas ¹	5	3
Within 30 nm of a sensitive site ²	4	2
Falls within outer perimeter of Class B airspace	3	1
Falls within the boundaries of restricted airspace	3	1
Level of Traffic		
Greater than 101 based aircraft	3	1
26-100 based aircraft	2	-
11-25 based aircraft	1	-
10 or fewer based aircraft	-	-
Based aircraft over 12,500 lbs	3	1
Runway		
Runway length greater than 5001 feet	5	3
Runway length less than 5000 feet, Greater than 2001 Feet	4	2
Runway length 2000 feet or less	2	-
Asphalt or concrete runway	1	-
Operations		
Over 50,000 annual aircraft operations	4	2
Part 135 operations	3	1
Part 137 operations	3	1
Part 125 operations	3	1
Flight training	3	1
Flight training in aircraft over 12,500 lbs	4	2
Rental aircraft	4	2
Maintenance, Repair, and Overhaul facilities conducting long term storage of aircraft over 12,500 lbs	4	2
Total		

Assess points for every characteristic that applies to your facility.

1. Mass population area - Area with a total metropolitan population of at least 100,000 people.
2. Sensitive sites - Areas which would be considered key assets or critical infrastructure of the United States. Sensitive sites can include certain military installations, nuclear and chemical plants, centers of government, monuments and iconic structures, and/or international ports.
3. Facilities with multiple runways should only consider the longest runway on the airport.
4. Airports at higher elevations may need longer runways to accommodate even the smallest of aircraft. It is not the intent of this document to assess points for a longer runway if it is unrealistic that the runway could be used for larger aircraft operations.

Appendix B – Suggested Airport Security Enhancements

Points/Suggested Guidelines			
>45	25-44	15-24	0-14
<ul style="list-style-type: none"> • Fencing (Section 3.3.3) • Hangars (Section 3.3.1) • CCTV (Section 3.4.5) • Intrusion Detection System (Section 3.4.6) 			
<ul style="list-style-type: none"> • Access Controls (Section 3.3.2) • Lighting System (Section 3.3.4) • Personnel ID System (Section 3.3.6) • Vehicle ID System (Section 3.3.5) • Challenge Procedures (Section 3.4.7) 			
<ul style="list-style-type: none"> • LEO Support (Section 3.4.4) • Security Committee (Section 3.5.2) • Transient Side Sign-in/Cut Procedures (Section 3.1.2) 			
<ul style="list-style-type: none"> • Signs (Section 3.3.5) • Documented Security Procedures (Section 3.5.1) • Positive Passenger/Cargo/Baggage ID (Section 3.1.1) • All Aircraft Secured (Section 3.2) • Community Watch Program (Section 3.4.1) • Contact List (Section 3.5.3) 			

Appendix C – Locks

Many ingenious methods have been developed to open locks surreptitiously. Some locks require considerable time and expert manipulation for covert opening but all will succumb to force and the proper tools. Further, many locks can be bypassed either because of poor construction of the lock, poor building construction, or improper installation.

Locks are an integral part of barriers and their security. In addition to their physiological deterrence, their physical strength and resistance to all but the most determined thief provides security in itself. In addition, the loss in time and usual added noise will give increased probability of detection.

It is important that the manager of a facility know each employee who has access to each lock. Key control is as important as the use of locks. There are various types of locks that may be employed at an airport:

- **Combination Locks** - Combination padlocks can be designed with either fixed or changeable combination mechanisms. However, care should be taken when employing these locks in an area exposed to the elements. Lock combinations should be changed regularly.
- **Cipher Locks** - A variety of cipher (push button) locks are available. The use of these locks should be limited to controlling access in manned areas as lock codes can be given to unauthorized users. Both electrical and mechanical cipher locks are available. Each may be used with electric release latches, and doors with this type of lock should be equipped with automatic door closers. The electrical cipher lock should also be equipped with a keyed bypass lock to allow access in the event of power failure. These lock codes should also be changed regularly.
- **Key Locks** - The key type padlock of brass construction with pin tumblers and a hardened shackle are generally the most satisfactory for outside use. Where possible, locks should be rekeyed, replaced, or discarded prior to a new tenant moving in.

Advanced electronic key technologies should also be considered. These systems provide a number of benefits to the user. First, electronic keys provide airport management with the ability to immediately disable access on keys that are lost or stolen. Second, using electronic keys provide a record of users movements throughout the airport area.

Deadbolt locks, built-in door handle locks, or padlocks and metallic keys should be considered to secure an access point, particularly those that are low-risk, low throughput, or significantly distant from the main areas of concern or from the central control station. Such locking systems may involve other procedural issues, such as a key management system and the difficulties of recoring at numerous locations and the reissuing of keys when they are lost or stolen.

Of primary importance in maintaining the integrity of a locking system is the establishment of effective key control, including control of keys, key codes, key cutting and combination equipment, and key issuance and retrieval. Rigid controls should be established to ensure that:

- If systems requiring key cutting codes and equipment are used, measures are taken to protect them against loss or misuse.
- Key issuance authority is limited to as few personnel as possible to minimize improper distribution.
- Keys are issued to personnel on the basis of operational needs and not as a convenience.
- Keys are retrieved when personnel leave the airport by transfer, dismissal, resignation, or lease expiration.
- Lost keys are reported promptly to the appropriate airport personnel.
- Unissued locks and keys are properly safeguarded.
- Keys are stamped or engraved with "Do Not Duplicate".
- The key issuance system is periodically audited to ensure accountability for all keys.

An important consideration in such investments in airport equipment is total life cycle costs, not merely the initial capital cost. This is a concept that should carry over into any equipment procurement process.

Appendix D – Fencing

Security fencing is the most common means of securing a perimeter. Fencing can vary in design, height, and type depending on local security needs. Typically, fences are low-maintenance, provide clear visibility for security patrols, and are available in varieties that can be installed in almost any environment. Barbed wire, razor wire, and other available features increase intrusion difficulty. For locations with aesthetic concerns, there are also a large variety of decorative yet functional styles available, as well as opaque styles that limit public visibility of service, storage, or other non-aesthetic areas.

Fencing can vary in design and function depending on the facility. Such barriers can range from chain link fencing topped with barbed wire similar to that found at commercial service airports, to a simple split rail fence designed to alert individuals to the presence of the airport operations area. In any case, fencing will not discourage a determined intruder. However, it can serve to alert airport management to the presence of unauthorized individuals. To derive value from a fencing system, airport personnel and users must be educated in the use of a “challenge” system. A challenge system involves airport employees and users confronting unknown personnel on the airport to determine whether or not they have a valid reason for being on airport property. Such a system may include stopping and questioning or even simply greeting the unknown individual and engaging in conversation to determine their purpose for being in a restricted area.

It should be noted that while fencing is normally the most effective physical barrier for securing the airside, fencing an entire perimeter may not be economically feasible or even necessary for many airports. Partial fencing of sensitive areas such as the terminal area, aircraft storage, or maintenance areas may be more appropriate and can prove to be just as effective.

The physical security barrier provided by a fence provides the following functions¹:

- Gives notice of the legal boundary of the outermost limits of a facility or security sensitive area.
- Assists in controlling and screening authorized entries into a secured area by deterring entry elsewhere along the boundary.
- Supports surveillance, detection, assessment, and other security functions by providing a zone for installing intrusion detection equipment and closed-circuit television (CCTV).
- Deters casual intruders from penetrating a secured area by presenting a barrier that requires an overt action to enter.

¹ Source: Chain Link Fence Manufacturer's Institute.

- c Demonstrates the intent of an intruder by their overt action of gaining entry.
- Causes a delay to obtain access to a facility, thereby increasing the possibility of detection.
- Creates a psychological deterrent.
- Optimizes the use of security personnel while enhancing the capabilities for detection and apprehension of unauthorized individuals.
- Demonstrates a corporate concern for facility security
- Provides a cost effective method of protecting facilities

Some basic fencing features that enhance security include:

- **Height** - the higher the barrier, the more difficult and time consuming to breach.
- **Barbed Wire** - adding barbed wire at the top of the fence increases the level of difficulty and time to breach.
- **Eliminating handholds** - omitting a rail at the top of the fence makes the fence more difficult to climb.
- **Burying the bottom of the fencing** - eliminates the possibility of forcing the mesh up so that individuals can crawl under.
- **Sensor system** - addition of an intrusion/alert system adds another level of security to the perimeter.
- **Lighting** - increases visibility as well as raises the level of psychological deterrent.
- **Signage** - installed along the fence line, signs are important to indicate private secured areas and the presence of security patrols, alarms, or monitoring systems.
- **Clear areas** - security effectiveness of perimeter fencing is materially improved by the provision of clear areas on both sides of the fence, particularly in the vicinity of the terminal and any other critical facilities. Such clearance areas facilitate surveillance and maintenance of fencing and deny cover to vandals and trespassers. Suggested clear distances range from 10 to 30 feet, within which there should be no climbable objects, trees, or utility poles abutting the fence line nor areas for stackable crates, pallets, storage containers, or other materials. Likewise, the parking of vehicles along the fence should also be minimized. In addition, landscaping within the clear area should be minimized or eliminated to reduce potential hidden locations for persons, objects, fence damage, and vandalism.

There have been cases in which individuals have gained access to passenger aircraft by scaling or crashing through perimeter fencing. To deter or delay attacks, sufficient distance should be maintained between the perimeter fencing and aircraft parking areas.

However, airport operators should be careful that increased perimeter controls and measures do not prevent authorized personnel from gaining airfield access (e.g. fire and emergency response vehicles and personnel need to be assured unrestricted access).

Additional information on materials and installation is available in FAA Advisory Circular (AC) 107-1, Aviation Security – Airports; AC 150/5360-13, Planning and Design Guidelines for Airport Terminal Facilities; AC 150/5370-10, Standards for Specifying Construction of Airports, and DOT/FAA/AR-00/52, Recommended Security Guidelines for Airport Planning, Design, and Construction.

Appendix E – Access Points

If perimeter controls are used for an airport, access points for personnel and vehicles through the boundary lines, such as gates, doors, and electronically controlled or monitored access points should also be considered. In addition, access point type and design may be the determining factor in the effectiveness of the security boundary and control in that area. So, in all cases, the number of access points should be minimized and their use and conditions regularly monitored.

Any access point through a fence or other boundary should not only be able to control or prevent access, but also differentiate between an authorized and an unauthorized user. At an airport, access through boundary lines is often quite frequent, and must be quick in order to prevent unacceptable delays. In addition, if a boundary access point is not user-friendly, it may be abused, disregarded, or subverted and thus pose a security risk. Regardless of boundary location or type, the number of access points should be minimized for both security and cost efficiency.

Gates are the only moveable part of a fence and therefore should be properly constructed with appropriate fittings. Chain link gate specifications are specified in industry and federal guidance documents listed in the bibliography. Gates should be constructed and installed to the same or greater standard of security as any adjacent fencing in order to maintain the integrity of the area. All gates should have self-closures and be equipped so that they can be secured should enhanced security conditions require it. All gates should be sufficiently lighted. Swing gate hinges should be of the non-liftoff type or provided with additional welding to prevent the gates from being removed. Security provided by gates can be improved if they are designed and installed with no more than 4-6" of ground clearance beneath the gate and minimal gaps on both sides of the gate.

For vehicle access, limiting the size of the opening increases security, reduces the possibility of one vehicle passing another and shortens the open close cycle time. The cantilever slide gate is the most effective for vehicle security especially one that is electrically operated and tied into an access control system.

"Tailgating" entry may be a concern at unstaffed vehicle access points. Tailgating involves an unauthorized vehicle closely following behind an authorized vehicle in order to pass through an access point before the gate closes. The first response to this is usually a procedural one rather than design, since it is the responsibility of the person authorized to use the gate to be certain tailgating does not occur. To reinforce the user's responsibility, the airport may elect to use signs reminding vehicle operators to confirm gate closure. However, if a fence design solution is desired, an automated two-gate system (also known as vehicle entrapment gate) is one method that can help prevent "tailgate" entry. Such gates are separated one vehicle length apart and are sequenced so that

the second gate does not open until the first has fully closed. Time-delayed closures are a viable alternative. Timers can be increased or decreased to accommodate threat levels. Sensor arrays have also been used to successfully monitor vehicle movement and assist in detection of "tailgate" entries. "Tailgating" and "reverse tailgating" (where a vehicle enters a gate opened by an exiting vehicle) at automated gates may also be reduced by use of a security equipment layout that provides space for waiting vehicles to stop, which obstructs, or at least deters other vehicles from passing through.

Pedestrian/personnel gates can be constructed using a basic padlock or designed with an electrical or mechanical lock or a keypad/card key system tied into an access control system. Pre-hung pedestrian gates/portals installed independent of the fence line are available to isolate the gate from fence lines containing sensor systems, thus reducing possible false alarms.

Appendix F – Lighting

Good protective lighting is achieved by adequate, even light upon bordering areas, glaring lights oriented toward pedestrian and vehicle avenues of approach, and relatively little light on the guard personnel. Lighting units for perimeter fences should be located a sufficient distance within the protected area and above the fence so that the light pattern on the ground will include an area on both the inside and the outside of the fence. Generally, the light band should illuminate the fence perimeter barrier and extend as deeply as possible into the approach area. Limiting factors on the orientation of lights and the depth of the light band may include airport operations and air safety requirements, residences, waterways, and roadways. Types of protective lighting systems and light sources include the following:

- **Continuous Lighting.** This is the most common protective lighting system. It consists of a series of fixed lights arranged to flood a given area with overlapping zones of light on a continuous basis during the hours of darkness. There are two methods of employment of this system:
 - Glare projection lighting where the glare of lights directed across surrounding territory will not be annoying or interfere with adjacent operations;
 - Controlled lighting where the width of the lighted strip is restricted to meet a particular need.
- **Standby Lighting.** Lights in this system are either automatically or manually turned on at a prearranged time, when suspicious activity is detected, or when an interruption of power occurs.
- **Movable Lighting.** This type of lighting consists of manually-operated, movable flood lights.
- **Emergency Lighting.** This system may duplicate any of the aforementioned systems. Its use is limited to periods of power failure or other emergencies and is dependent upon an alternate power source.
- **Solar Powered Lighting:** In areas where electricity does not exist or is cost prohibitive solar powered lighting may be considered a viable alternative and have a wide range of applications.

Lighting of security areas on both sides of gates and selected areas of fencing is highly effective. Lighting is beneficial not only for security inspection, but also to ensure that fence/gate signage is readable and that card readers, keypads, phones, locks, and/or other devices at the gate are visible and usable. Similarly, sufficient lighting is required for any area in which a CCTV camera is intended to monitor activity. Reduced lighting or sensor activated (e.g. proximity, photoelectric, or timers) lighting may be considered in areas which have minimal traffic throughput in the off-peak hours.

Appendix G – Security Procedures Template

GA Airport Security Procedures

(Airport Name)

(Original Publication Date)

(Date Last Revised)

Table of Contents

Outline all of the sections of the document with corresponding page number for quick reference.

Section I: Disclosure Statement / Security Responsibilities

Distribution of these Security Procedures should be restricted to individuals with a legitimate need for access to them.

Identify the individual who has the responsibility for the development, upkeep and administration of the Airport Security Procedures

Section II: General Information

1. Forward

Identify the airport owner and the person(s) responsible for airport activities (e.g. State, county, authority, commission).

2. Introduction and Purpose

Provide a brief introduction that describes the purpose (what will it be used for) and the need (why was it created) for airport security procedures.

3. Distribution

You should list all individuals and agencies that will receive copies of the Airport Security Procedures.

Example:

- State / Local Police Department
- Fixed Base Operator
- Individual Tenants

4. Name and Location of Airport

- Airport Name
- Airport Address
- Normal Business / 24-hour Emergency / Fax Phone Number
- Airport Identifier
- Proximity to nearest major city. List the city and provide a state location map as an attachment.
- Airport Geographical Coordinates: latitude, longitude, elevation.

5. Airport Activities

- Types of flight activities (e.g. flight school, State Police, corporate)
- Hours of operation
- Number of annual operations
- Number of based aircraft

6. Airport Description

- **Size:** List the size of the airport in approximate acres or square miles.
- **Runways, Taxiways, Ramps:** Identify runways and their dimensions, taxiways, and ramp areas: Provide an airport layout plan / diagram as an attachment.
- **Buildings:**
 - List the number and types of buildings (offices, hangars, maintenance shops).
 - List the primary tenants for each of the buildings.
- **Airport Tenants:**
 - List hours of operation
 - List primary and emergency contact information
- **Other Airport Facilities**

7. Emergency Phone Numbers:

List all appropriate emergency contact numbers. Include point of contact names and office hours of operation as appropriate (e.g. FSD, alternate contacts).

- All Emergencies 911
- State Police (non-emergency)
- Local Police (non-emergency)
- Local Fire Department
- Airport Director (24 hour contact)
- Airport Facility Supervisor (pager)
- State / Local Aviation Official
- Federal Bureau of Investigation Local Field Office
- FAA Flight Standards District Office (FSDO)
- TSA Airport Watch Hot-Line 866-427-3287
- Local TSA Federal Security Director

Section III: Definitions and Terms

It may be useful to include a list of frequently used terminology to enhance clarity within the document.

Section IV: Administration

1. Airport Operator: List who operates the airport.
2. Individual responsible for airport security

List the responsibilities of this individual. These duties may include:

- Timely provision of evidence of security measure compliance as may be requested.
- Maintaining a complete and current list of all individuals with airport access.
- Maintaining documentation of all training provided in accordance with any current Airport Security Procedures.
- Maintaining and updating the Airport Security Procedures to reflect the current state of conditions at the airport.
- Timely distribution of the Airport Security Procedures or specific parts thereof, to appropriate persons or entities.
- Proper dissemination of all correspondence or other communications with airport tenants and others on security related matters.
- Daily oversight of security provisions at the airport and ensuring compliance with the Security Procedures.

Section V: Aircraft Movement Area / Security Control

1. Aircraft Movement Area
Describe any area that may be used for landing, take-off, and surface maneuvering of aircraft including all intermediate unpaved sections of the airfield encompassed on the airport property. You should also include a map or diagram as an attachment.
2. Describe any perimeter barriers or access controls such as:
 - Fencing
 - Gates
 - Access Control System
 - Airport Locks
 - Key Control System

Section VI: Airport Security Procedures

Describe any Airport Security Procedures such as:

- Aircraft security requirements
- Pedestrian/vehicle access
- Challenge procedures
- Reporting of suspicious behavior

Section VII: Airport Emergency Grid Map

Airport operators may also wish to consider creating an emergency locator map. The map should identify all relevant areas of the airport on a grid map such as:

- Runways
- Ramp areas
- Fence line
- Gates
- Automobile parking areas
- Hydrants
- Emergency shelters
- Buildings
- Hazardous materials sites

This map should be provided to emergency response personnel (fire, EMS, etc.) and law enforcement as well as airport personnel.

Section VIII: Identification of Airport Personnel

Describe any personnel identification methods/systems and the procedures for those that are currently in use. Such as:

- Airport-issued identification badge(s) or card(s)
- Identification Badge / Card application procedures
- Other acceptable forms of identification
- Accountability of lost/stolen identification badges / cards
- Temporary airport identification badges / cards
- Uniforms which display logo or other identifiable markings

Section IX: Identification of Vehicles

Describe what methods/systems are used to identify authorized vehicles in the air operations area. The following are examples of methods to identify authorized vehicles:

- Special paint schemes or markings
- Decal in a specified location on the vehicle
- Hang tags

Section X: Law Enforcement

Describe any agreement(s) and responsibilities that the airport owner/operator(s) may have with law enforcement agencies to provide support, traffic control, police patrols and any emergency responses. Include any written agreements as attachments to the Airport Security Procedures.

Also include any methods or systems used (e.g. radios, communications channels, etc.) to directly communicate with law enforcement personnel.

Section XI: Special Events

Describe any procedures that exist for special events such as:

- Air shows
- VIP Visits
- Events that result in unusual numbers of people on the airport.

Section XII: Increased Security Threats

Describe how security measures are implemented in accordance with the raising and lowering of the Homeland Security Advisory System as described in this Information Publication in Section 3.5.2.

Section XIII: Aviation Security Contingency Plans

Identify and describe all contingency plans and procedures established for security incidents such as:

- Bomb Threats (Bomb Threat Checklist is provided as an example)
- Civil Disturbances & Crowd Control
- Air Piracy (Hijacking) Actual or Attempted
- Suspicious/Unidentified Items

Bomb Threat Call Checklist

Fill out completely, immediately after bomb threat

Exact wording of the threat:						
Questions to ask:						
When is the bomb going to explode?						
What kind of bomb is it?						
What will cause it to explode?						
Did you place the bomb?						
Why?						
What is your address?						
What is your name?						
Sex of caller		Age		Race		Length of call
Caller's voice (circle all that apply):						
Calm	Laughing	Lisp	Disguised	Angry	Crying	Raspy
Accent	Excited	Normal	Deep	Slow	Distinct	Ragged
Slurred	Nasal	Soft	Loud	Stutter	Clearing Throat	
Deep Breathing		Cracking Voice		Other:		
If voice was familiar, whom did it sound like?						

Appendix H - Bibliography

This document provides numerous references and citations to other government and industry sources. These are not intended to be modified by this document in any way, and are generally intended to refer to the most current version of such external resources, to which the reader should go for detailed information.

FAA Advisory Circulars

The latest issuance of the following advisory circulars may be obtained from the Department of Transportation, Utilization and Storage Section, M-443.2, Washington, D.C. 20590: [Also see the FAA internet web site at www.faa.gov]

1. 00-2, Advisory Circular Checklist - Contains a listing of all current advisory circulars.
2. 107-1, Aviation Security-Airports - Provides guidance and recommendations for establishing and improving airport security.*
3. 108-1, Air Carrier Security. Provides information and guidance on the implementation of Airplane Operator Security.*
4. 109-1, Aviation Security Acceptance and Handling Procedures-Indirect Air Carrier Security. Provides guidance and information for use by indirect aircraft operators when accepting and handling property to be carried by aircraft operators or by the operator of any civil aircraft for transportation in air commerce.*
5. 129-3, Foreign Air Carrier Security. Provides information and guidance on the implementation foreign air carrier security.*
6. 150/5200-31A, Airport Emergency Plan
7. 150/5300-13, Airport Design
8. 150/5360-13, Planning and Design Guidelines for Airport Terminal Facilities. Furnishes guidance material for the planning and design of airport terminal buildings and related facilities.
9. 150/5370-10, Standards for Specifying Construction of Airports

* - On November 19, 2001, Congress enacted the Aviation and Transportation Security Act (ATSA), Public Law 107-71, 115 Stat. 597, which established the TSA. Pursuant to ATSA, the TSA became responsible for security in all modes of transportation, including civil aviation under Chapter 449 of title 49, United States Code, related research and development activities, and other transportation security functions exercised by DOT. Consequently 14 CFR parts 107, 108, 109, and certain provisions of part 129 were removed and transferred into the relevant parts of 49 CFR 1542, 1544, 1548, and 1546 respectively. While the materials referenced here are related to superceded regulations, they may still provide relevant information and have therefore been included.

U.S. Government Regulations

The TSA issues and administers Transportation Security Regulations (TSRs), which are codified in Title 49 of the Code of Federal Regulations (CFR), Chapter XII, parts 1500 through 1699. Many TSRs are former rules of the Federal Aviation Administration (FAA) that were transferred to TSA when TSA assumed FAA's civil aviation security function on February 17, 2002. [All of these regulations can be found at <http://www.tsa.gov/>].

It should be clearly noted that these regulations pertain mainly to regulated entities and not typically to GA operators or facilities and are provided for reference and informational purposes only.

1. **49 CFR Part 1540 Civil Aviation Security: General Rules** - This part contains rules that cover all segments of civil aviation security. It contains definitions that apply to Subchapter C, and it contains rules that apply to passengers, aviation employees, and other individuals and persons related to civil aviation security, including airport operators, aircraft operators, and foreign air carriers.
2. **49 CFR Part 1542 Airport Security** - This Part requires airport operators to adopt and carry out a security program approved by TSA. It describes requirements for security programs, including establishing secured areas, air operations areas, security identification display areas, and access control systems. This Part also contains requirements for fingerprint based criminal history record checks of specified individuals. This part describes the requirements related to Security Directives issued to airport operators.
3. **49 CFR Part 1544 Aircraft Operator Security: Air Carriers and Commercial Operators** - This Part applies to certain aircraft operators holding operating certificates for scheduled passenger operations, public charter passenger operations, private charter passenger operations, and other aircraft operators. This Part requires such operators to adopt and carry out a security program approved by TSA. It contains requirements for screening of passengers and property. This Part also describes requirements applicable to law enforcement officers flying armed aboard an aircraft, as well as requirements for fingerprint based criminal history record checks of specified individuals. This Part describes the requirements related to Security Directives issued to aircraft operators.
4. **49 CFR Part 1550 Aircraft Security Under General Operating and Flight Rules** - This part applies to the operation of aircraft for which there are no security requirements in other Parts of Chapter XII, including general aviation aircraft.

Other Reports

1. Recommended Security Guidelines for Airport Planning, Design and Construction, DOT/FAA/AR-00/52, Federal Aviation Administration, June 2001.

2. Report of the GA Airports Security Working Group, Aviation Security Advisory Committee, October 1, 2003.
3. GA Airport Security Task Force Recommendations, American Association of Airport Executives, June 2002.
4. GA Security, National Association of State Aviation Officials, December 2002.

Appendix I – Useful Websites

Aviation Trade Associations

Organization	Website
Aircraft Owners and Pilots Association	www.aopa.org
Airports Consultants Council	www.acconline.org
American Association of Airport Executives	www.aaae.com
Experimental Aircraft Association	www.eaa.org
GA Manufacturers Association	www.gama.aero
Helicopter Association International	www.rotor.com
National Agricultural Aircraft Association	www.agaviation.org
National Air Transportation Association	www.nata-online.org
National Association of State Aviation Officials	www.nasao.org
National Business Aviation Association	www.nbaa.org
United States Parachute Association	www.uspa.org

Federal Government

Organization	Website
Department of Homeland Security	www.dhs.gov
Federal Aviation Administration	www.faa.gov
Federal Bureau of Investigation	www.fbi.gov
Transportation Security Administration	www.tsa.gov

Other References

Organization	Website
ASIS International (Industrial security organization)	www.asisonline.org
Aviation Crime Prevention Institute	www.acpi.org
Chain Link Fence Manufacturers Institute	http://codewriters.com/asites/main-pub.cfm?usr=clfma

APPENDIX B

Advisory Committee and Technical (Task Force) Committee Members

ADVISORY COMMITTEE

Jerry L. Allen, A.A.E.
Director, Planning & Development
Palm Beach County
Department of Airports
846 Palm Beach International Airport
West Palm Beach, FL 33406
Phone: 561-471-7423

Cynthia Barrow
Executive Director
Bartow Municipal Airport
P.O. Box 650
Bartow, FL 33831
Phone: 863-533-1195

Edward Cooley, III, A.A.E.
Sr. Director of Operations/Public Safety
Hillborough County Aviation Authority
P.O. Box 22287
Tampa, FL 33622-2287
Phone: 813-870-8711

Angela Gittens
Director
Miami-Dade Aviation Department
P.O. Box 592075
Miami, FL 33159
Phone: 305-876-7077

Ericson W. Menger
Airport Director
Vero Beach Municipal Airport
P.O. Box 1389
Vero Beach, FL 32961-1389
Phone: 772-978-4930

Peter B. Modys, A.A.E.
Division Director - Aviation
Lee County Port Authority
16000 Chamberlin Parkway
Suite 8671
Ft. Myers, FL 33913-8899
Phone: 239-768-4312

Rob Pruitt
Director
Ocala International Airport
3400 S.W. 60th Avenue
Ocala, FL 34478
Phone: 352-629-8377

Gary Quill
Executive Director
Charlotte County Airport
28000 Airport Road, A-1
Punta Gorda, FL 33982
Phone: 941-639-1101

Elisa Newberry Rohr
Manager of Governmental Relations
Greater Orlando Aviation Authority
One Airport Blvd.
Orlando, FL 32827
Phone: 407-825-2092

G. Kelly Rubino
President
MEA Group, Inc.
MEA Business Center
9015 Towncenter Parkway, Suite 105
Lakewood Ranch, FL 34202
Phone: 941-342-6321

Charles H. "Chip" Snowden, Jr., A.A.E.
Chief Operating Officer
Jacksonville Airport Authority
Box 18018
Jacksonville, FL 32229-0018
Phone: 904-741-2070

Edward R. Wuellner, A.A.E.
Executive Director/Airport Manager
St. Augustine/St. Johns County Airport
Authority
4796 US 1 North
St. Augustine, FL 32095
Phone: 904-825-6860

Representing
Florida Department of Law Enforcement (FDLE)
Steve Lauer, Chief
Florida Domestic Security Division
Florida Department of Law Enforcement
2331 Phillips Road
Tallahassee, FL 32302
Phone: 850-410-8619

Representing
Transportation Security Administration (TSA)
Steven Calabro
Security Specialist – TSA Headquarters
601 S. 12th St. East Tower
11th Floor - TSA -7
Arlington, VA 22202
Phone: 571-227-2264

→ → →

Model Airport Security Plan Task Force Members

Bill Johnson, Project Manager

Executive Director
Florida Airports Council
1801 North Meridian Road
Tallahassee, FL 32303

**Jason Milewski – Technical Advisory
Committee Chair**

Airport Director
Sebastian Municipal Airport
1225 Main Street
Sebastian, FL 32958

**Peter Modys – President, Florida
Airports Council**

Division Director – Aviation
Lee County Port Authority
16000 Chamberlin Parkway
Suite 8671
Fort Myers, FL 33913

Cynthia Barrow

Executive Director
Bartow Municipal Airport
P.O. Box 650
Bartow, FL 33831

Mike Cavello

Palatka - Kay Larkin Municipal Airport
4015 Reid Street, Highway 100
Palatka, FL 32177

Bill Crouch

Independent Aviation Consultant
8277 NW 3rd Place
Coral Springs, FL 33071

Gary Duncan

Assistant Director
Lee County Port Authority
16000 Chamberlin Parkway
Suite 8671
Fort Myers, FL 33913

Mary Maher

Superintendent, Orlando Executive
Airport
Greater Orlando Aviation Authority
501 Herndon Avenue, Suite G
Orlando, FL 32803

George Manion

Manager, General Aviation Airports
Miami-Dade Aviation Department
14201 N.W. 42nd Avenue
Opa-Locka, FL 33054

Ericson Menger

Airport Director
Vero Beach Municipal Airport
P.O. Box 1389
Vero Beach, FL 32961

Rob Pruitt

Director
Ocala International Airport
3400 S.W. 60th Avenue
Ocala, FL 34478

Jim Werme

Airport Manager
Zephyrhills Municipal Airport
39450 South Avenue
Zephyrhills, FL 33540

APPENDIX C

FAC Phase One Report

**Phase One Report
February 25, 2004**

PREFACE

On September 30, 2003, the Florida Department of Transportation (FDOT) entered into an Agreement with the Florida Airports Council (FAC) to initiate the second year of a five-year master plan to strengthen the role of the state's airports in economic development. Airport managers throughout the state indicated that airport security was essential to each community's acceptance of their airport. The scope of the second-year study is to develop recommendations for coordinated security at Florida's commercial service and general aviation airports and to prepare a model airport security plan for general aviation airports. In addition, the Council is to develop recommendations on necessary state and/or federal legislation needed, and develop recommendations for funding needed to implement the plan.

TASK 1.1

The Study Phase required the establishment of an advisory committee that would consist of general aviation and commercial service airport professionals, along with state and federal officials, to oversee the study process. A list of the advisory committee members is provided as Attachment "A". In addition, the Council formed a Task Force of the General Aviation Committee to serve as the project's technical committee in preparing the Model GA Security Manual. The membership of the Task Force is provided as Attachment "B". Finally, security experts at Florida's commercial service airports were identified and used as resources for the project. Attachment "C" is a list of the security contacts at these airports.

TASK 1.2

Task 1.2 required the study team to review findings of previous surveys by FDOT and FDLE regarding airport security and conduct a new written survey of Florida's airports to determine the current status of security plans, procedures and key issues related to security and security coordination and determine the differences in requirements for general aviation and commercial service airports.

The Task Force contacted both FDOT and FDLE regarding previous surveys and only FDLE had completed a security survey following the terrorist attacks of September 11, 2001. According to FDLE, their survey was conducted by Florida Sheriffs and only asked four questions:

1. Do flight instructors allow students to preflight aircraft without supervision prior to final licensing?
2. Does the airfield require aircraft owners to secure aircraft from theft in any manner?
3. Does the airfield maintain any secure fenced area around aircraft or hazardous material (fuel)?
4. Does the airfield maintain any form of security identification check for entry to the flight line, aircraft parking area, fuel storage, or any flight operations area?

FDLE indicated it could not disclose the results of the survey but given the general nature of the survey, the technical committee felt it was of little use in developing a security manual for general aviation airports.

Security Survey

The Task Force prepared a survey that was sent to every public general aviation airport in Florida with the intent of determining which airports had current airport security plans (ASP's) and to determine which airport plans could be used as input for the model plan.

Surveys were forwarded to both publicly-owned and privately-owned general aviation airports. After a two-week response period, the Task Force attempted to contact each unresponsive airport manager and conducted a telephone survey with those that were available and willing to discuss GA security.

Analysis of Responses

Surveys were sent to 110 airports with 93 responses. The surveys indicated that the majority of GA airports in the state have not prepared security plans, with many indicating they are awaiting direction from the federal government.

The major security concern expressed by airport managers was unauthorized access to the airport/secure areas and the major security enhancements needed to address this were described as: better fencing and security gates. The survey also indicated that many airports have fencing projects planned within the next five years. Privately-owned airports that are open to the public do not currently receive state or federal funds and they indicated such funds would be necessary for them to be able to fence and secure their airports.

One area that became apparent during telephone interviews with the privately-owned airports was the high level of security at these airports because each of these airports, with the exception of one, has security personnel that reside on the property. These security personnel are familiar with each based aircraft owner and questions transient aircraft owners on their intentions. Public airports could benefit from on-property security, as well. In some cases, local land-use ordinances may need to be changed to allow this to happen.

A large number of airports voiced their concern that the state not promulgate regulations governing security of GA airports and that any proposals developed by this study be in the form of guidelines only.

Commercial Service Airport Security vs. General Aviation Airport Security

Proviso language in the bill authorizing this study indicated a concern to coordinate security at Florida's commercial service and general aviation airports. Security at these two different category airports could not be more dissimilar. The federal government has stringent regulations governing security at airports serving commercial airlines and is currently determining its role governing security of general aviation airports.

History

The Aviation and Transportation Security Act, Public Law 107-71, enacted into law on November 19, 2001, established the Transportation Security Administration (TSA) as a new

operating administration within the Department of Transportation. On Nov. 25, 2002, President George Bush signed the Homeland Security Act which created the Department of Homeland Security. On March 1, 2003, TSA, the Coast Guard, Secret Service, INS and Customs were transferred into the Department of Homeland Security. By June 1, 2003, a total of 22 agencies were transferred into the Dept. of Homeland Security.

FAR Part 107

Prior to the Transportation Security Act and the creation of the TSA, FAR Part 107 prescribed rules for airport operators servicing and facilitating U.S. certificated air carriers, foreign air carriers, and both foreign and domestic air cargo carriers. The purpose of Part 107 was to prevent any act of unlawful interference with the safety of persons and goods in the air. In order to accomplish this, the FAA extended its security regulations to airports as the first practical line of defense.

There were four key security elements required under FAR Part 107; prepare and implement an airport security plan; provide for the presence of law enforcement and their response through an alerting system; implement limited controlled access to secured areas; and, to provide for a system of identification and recognition of persons and vehicles. The full requirements of Part 107 applied to air carrier airports served by aircraft having seating capacities of greater than 60 seats. Parts of 107 applied to airports served by air carriers with seating capacity between 30 and 60 seats, and did not apply to airports being served by air carriers with less than 30 seats.

During the time FAR Part 107 was in effect, the FAA was not involved in implementing or requiring any type of security related measures for general aviation airports. Neither the FAA or airport operators deemed general aviation aircraft as a security threat.

Immediately following the terrorist attacks, Secretary of Transportation, Norman Y. Mineta, wrote to the Honorable Don Young, Chairman of the Committee on Transportation and Infrastructure, U.S. House of Representatives regarding general aviation security and concluded that, "general aviation is a critical component of the Nation's transportation system. We must continue to develop, assess and deploy measures that can effectively increase the security of general aviation without unduly restricting general aviation operations. Such measures can be deployed singly or in appropriate combination in response to varying threat levels."

TSA and 49 CFR Part 1542

Soon after the attacks, Congress passed the Aviation and Transportation Security Act, TSA was created, and 49 CFR Part 1542 was adopted into law, eliminating the FAA from overseeing airport security and eliminating FAR Part 107.

TSA evaluated all potential threats associated with the different forms of aviation as well as looking at and improving security as it related to all forms of transportation. However, the immediate and largest impacts affected commercial aviation. Cockpit doors are now hardened and secured and airline pilots, after being adequately trained, have been allowed to carry firearms onto the planes. TSA, with over 45,000 federal employees, screens all luggage utilizing some form of electronic scan or trace detection and also screens all passengers at all of the nations 429 commercial airports.

Although the TSA was tasked with improving all forms of transportation security, including air cargo and general aviation, the emphasis has been on commercial aviation – where the September 11th attacks originated and where the federal government felt the greatest threat continued to lie.

General Aviation Security

TSA's mission for general aviation security is to enhance the security of the general aviation community by developing guidelines and encouraging voluntary compliance. TSA recognizes that one size does not fit all when it comes to general aviation security. They also recognize that any recommendations will come at a huge expense.

After the terrorist attacks, the government immediately suspended, revoked or refused to issue airmen certificates to anyone that the TSA determined posed a threat. Background checks are now required on individuals seeking to receive a U.S. pilot certificate on the basis of a foreign pilot certificate and all pilots must carry government-issued photo identification. The FAA also began issuing new, security enhanced airman certificates with an FAA hologram seal on it. These certificates will be issued to all new and existing airmen as they achieve a higher or additional rating. TSA worked with the Aircraft Owners and Pilots Association (AOPA) and developed the Airport Watch Program which was based on successful neighborhood watch programs. To date, TSA has not required any additional regulation for general aviation airports, however, there are changes being discussed.

TSA is actively working to evaluate risk factors associated with GA airports. GA vulnerability assessments will be identified and common threats evaluated. Protective measures will be recommended and regulatory directions, if any, will be determined. The concern amongst GA airport operators is "Who will pay....who will pay to perform the assessment, and who will pay for the improvements?" Many GA airports operate in the red and could not afford to implement a costly security program or install costly security related equipment to chase or protect against a threat that may not exist without considerable financial support of the state and/or federal government.

AOPA's Airport Watch Program

The Airport Watch Program advises pilots to:

- Always carry a government-issued photo ID
- Be cooperative with airport security and management
- Share information on your aircraft and other pilots authorized to use it
- Get to know your airport community
- Greet strangers
- Stand united with other airport users through regular meetings
- Have tools ready such as cellular telephones to advise management of suspicious activities
- Spread the word about Airport Watch
- Be prepared for the long-haul. Airport awareness will be a permanent job for pilots using airports throughout the country.

Pilots are advised to call 911 in an emergency situation and to call the National Response Center at 1-866-GA-SECURE to report suspicious activity. Pilots are advised to secure their aircraft

whenever not in use, whether they are in a hangar or outside. Auxiliary locks are recommended as an extra line of defense. Finally, AOPA advises its members, "*When in doubt, check it out!*"

Task 1.3 – Review of Benchmarks and Supporting Data

Task 1.3 required a review and analysis of models for general aviation security including benchmark airports. This review was undertaken by the Task Force at a meeting on December 3rd in Ocala, Florida. The group reviewed information provided by other states, TSA, FAA, AOPA, a draft of the ASAC White Paper and benchmark airport plans. The meeting resulted in a preliminary draft of an outline for a GA airport security plan which will be reviewed by airports, local and state officials in January and February, 2004. On December 4th, the Advisory Board met in Tampa, Florida and was briefed on the status of the project by members of the Task Force.

Issues of Concern to Florida's GA Airport Managers

The Task Force discussed the major concerns expressed by Florida's airport community, which included:

- Theft of aircraft
- Vandalism of aircraft and airport property
- Lack of proper/adequate fencing and gates
- Lack of adequate lighting
- Lack of personnel to monitor airport security
- Hangar access security
- Inadequate controls on vehicular access
- Fear of excess regulation by federal or state government
- Public perception of aircraft role in terrorist attacks and resultant public perception of aviation's role in future terrorist attacks
- Abuse of existing gate-card systems
- Uncontrolled airspace
- Fuel farm security
- Hangar security
- Inadequate funding for security projects or staffing
- Lack of tenant understanding/support for airport security
- Inability to visually identify pilots/authorized airport users
- Lack of guidelines from TSA or FAA
- Lack of signage guidance
- Loss of business after 9/11

Private airport owners indicated their concerns also included:

- Governmental interference
- Lack of state funds for private airport security enhancements

Secondly, the Task Force discussed recommendations made by airport managers, which were:

- Keep the plan simple
- Develop a funding plan for fencing and access control standard for all GA airports

- Be affordable for GA airports
- Take advantage of existing police, sheriff assets
- Consider contract towers as a security asset
- Consider video surveillance opportunities
- Consider minimum personnel recommendations
- Consider badging systems
- Provide better communications between airport management and tenants and users.
- Enhance the airport without being too expensive
- Guidelines to be advisory and not regulatory

Airport managers overwhelmingly felt that GA airports were not security threats but that safety and security could be enhanced to benefit the flying public.

Other State Programs

In an effort to determine what other states had done in the area of GA security, the Task Force contacted the National Association of State Aviation Officials (NASAO) who recommended contacting aviation directors in Virginia, Massachusetts, New York, California, New Jersey, and Missouri. States directly impacted by the terrorists attacks (New York, Massachusetts) have been the most aggressive in dealing with airport security and GA airport security was and continues to be an issue of concern for these states. Now that more than two years have passed since the attacks, concern over GA security has become less of a national issue and the majority of states are awaiting direction from the TSA.

The State of Virginia was, in fact, currently pursuing the development of security plans for GA airports in the state through a contract with a consulting firm. A copy of their RFP was reviewed and portions will be incorporated into Florida's Model Plan.

The State of Massachusetts, because two of the airliners used in the September 11th attacks originated in the state, was the most aggressive pursuing aviation regulation. One positive action taken by the state was development of a secure website for airport managers to receive the latest security information from the state. One questionable action taken was the state's requirement that all aircraft owners, pilots, and airport 'users' be issued badges. Airport managers throughout the state were delegated the responsibility of issuing the badges.

The State of New Jersey enacted a two-lock rule that requires aircraft to have a secondary lock, such as a propeller or throttle lock, to aid against theft. They also produced signage for all airports on airport security and issued digital pagers to all airport managers for better communications between the State and each airport manager. They also provided wallet cards for all airport users with federal and state contacts and telephone numbers.

Missouri published "Security Guidance for General Aviation Airports" which was reviewed by the FAC Task Force for incorporation into Florida's Model Plan. Of particular interest to the committee is their categorization of airports based on runway length.

The State of New York, for obvious reasons, was also very aggressive in providing directions to its GA airports and a copy of their best practices manual was considered as an excellent guide for Florida's manual.

Benchmark Airport Programs

Several GA airports in Florida prepared security plans for their facilities in an effort to be proactive. Each of these plans is based on that airport's perception of security concerns. Without federal (or state) guidance, these plans vary widely.

Each of these airport plans has been reviewed by the Task Force and the model Security Manual, to be prepared in Phase II of this study, will be an amalgam of these plans – incorporating the best ideas from each. The airports that had developed security manuals focused on: security of the aircraft operations area (AOA); tenant security, and special-use operations – such as banner towing and skydiving. Each had developed emergency contact lists for local, state, and federal agencies, as well.

Several airports (Jacksonville, for example) developed a tiered security system based on TSA's color system. Sebastian Municipal Airport had the most comprehensive definitions section which all agreed would be included in the final model manual. Sebastian had also determined that a comprehensive security badging system was a goal of their plan. As in the case of Massachusetts, Task Force members felt a compulsory badging system, managed by each airport, may be beyond the capabilities of many airports in Florida. The Task Force agreed to discuss the pro's and con's of compulsory badging at future meetings.

The group also reviewed a model program undertaken by Zephyrhills, through a contract with FDOT, that also included a security component and agreed that FDOT should not issue additional grants to individual airports until the Model Plan was completed.

Two issues discussed and not resolved were: (1) Whether FDOT should mandate that each airport have some level of security plan to be able to receive state funds and (2) whether trespassing on airport property continues to be a misdemeanor or be a felony. It was felt that once the model plan was completed, each airport could easily develop a plan with its internal resources or with assistance from the Florida Airports Council and/or FDOT. As to the second issue, it was brought to the attention of the group that trespassing on an airport is considered a misdemeanor and the group felt that, after September 11th, airport trespassing may need to be strengthened to a felony. All agreed that these issues needed more discussion in future phases of the study prior to making a final recommendation.

ASAC Report

TSA formed the Aviation Security Advisory Committee (ASAC) comprised of industry professionals to make recommendations on aviation security-related issues. Working Groups were developed to explore general aviation airport security and air cargo security.

The GA Airport Security Working Group consists of representatives from a diverse group of aviation industry representatives, including:

- Aircraft Owners & Pilots Association (AOPA);
- Airport Consultants Council (ACC);
- American Association of Airport Executives (AAAE);
- Experimental Aircraft Association (EAA);
- General Aviation Manufacturers Association (GAMA);
- Helicopter Association International (HAI);

- National Air Transportation Association (NATA);
- National Association of State Aviation Officials (NASAO);
- National Business Aviation Association (NBAA); and
- United States Parachute Association (USUA).

Ex Officio members of the Working Group includes representatives of the Federal Aviation Administration (FAA) and TSA.

The Transportation Security Administration has been awaiting this report and has advised the industry that it will issue GA Security "Guidelines" by mid-2004. The TSA indicated that it "will build on these recommendations to establish formal guidelines that general aviation airports can follow to further strengthen security" at some 18,000 general aviation airports or landing facilities in the U.S.

The report is intended to be a document that the TSA can circulate to state government aviation agencies, airport operators and managers, and airport businesses as they consider implementing appropriate security measures at general aviation airports.

Intrinsic in the guidelines is the concept that each general aviation airport is unique. As a result, the Working Group went to great lengths to make their recommendations relevant to each airport or landing area, whether it is adjacent to a major metropolitan area or rural community. Accordingly, the Working Group closely considered but could not reach consensus on various proposals to "categorize" general aviation airports as a way of prescribing which, if any, of these recommendations should be implemented at which airports. Similarly, other characteristic-based methods to apply some but not other recommendations to specific airports and landing facilities were discarded.

Key Findings of the Report

- The Working Group made recommendations in the following areas:
 - Pilots and Passengers
 - Security of Aircraft
 - Airports and Facilities
 - Surveillance
 - Security Plans and Communications
 - Specialty Operations
- Unfunded mandates to airports, states, general aviation businesses, manufacturers and pilots should be avoided.
- General aviation is but one aspect of the nation's transportation system. It should not be "isolated" and asked to follow security procedures that are beyond those being adopted as "best practices" by other transportation modes.
- GA airports are extremely diverse; appropriate security measures can only be determined by careful examination of an individual airport.
- There is a distinct difference between "public use" airports and "private use" airports. Privately-owned, private-use GA airports receive no public funds and most state government

aviation agencies have no authority to regulate them. Beyond this distinction, the group was unable to reach consensus on further airport categorization. However, the group agreed that it would be willing to reconvene, at the invitation of TSA, to examine any categorization plan brought forward in the future.

In addition to the recommendations and key finding, the Working Group also made the following recommendations to the federal government.

Credentialing

- First time applicants should be required to show a government issued photo ID to prove their country of citizenship before obtaining a U.S. pilot certificate.
- The FAA Pilot Certificate should be modified to include a photograph of the pilot using a format that is difficult to counterfeit.

Security Response Procedures

- Develop procedures and/or a system to communicate appropriate general aviation security and/or threat information to potentially affected general aviation entities.

Reward Program

- Recommend that the TSA establish a terrorism prevention reward program for general aviation airports.

Federal Funds for Hangar Construction

- Federal, state, and local dollars should be encouraged towards hangar construction to secure aircraft and improve airport facilities. Legislation allowing this is awaiting final approval in the Conference Report accompanying the FAA reauthorization legislation (H.R. 2115).

The Task Force agreed that since the Transportation Security Administration was considering the recommendations of the ASAC Working Group to be the consensus of the aviation industry and would be incorporated into TSA's final recommendations, this report would also be considered in development of Florida's Model Plan.

Summary

Due to the lack of regulation on general aviation security, GA airports around the nation have been forced to create their own security programs that are based on the personal experiences and values of each airport management team. As evidenced by the survey, many GA airports have not developed security programs and are awaiting direction from the federal government.

The Model Security Manual to be developed as a part of this project will provide guidance for all GA airports as to what programs should be considered. It is expected that airport managers will adopt measures and programs they feel are financially feasible as well as practical for their size and type of airport.

Upon completion of the Model Security Manual, workshops will be scheduled to discuss programs outlined in the plan with airport managers from throughout the State of Florida.

✈ ✈ ✈

APPENDIX D

Report of the
Aviation Security Advisory Committee Working Group
On
General Aviation Security

**Report
Of The
Aviation Security Advisory Committee Working Group
On
General Aviation Airports Security**

Purpose of this Report

The Transportation Security Administration (TSA) requested the Aviation Security Advisory Committee (ASAC) establish a Working Group made up of industry stakeholders to develop guidelines for security enhancements at the nation's privately and publicly owned and operated general aviation (GA) landing facilities. This listing of recommended guidelines or "best practices" is designed to establish non-regulatory standards for general aviation airport security.

The Working Group represents the overwhelming majority of those engaged in the general aviation industry on the important issue of ensuring the continued security of the nation's general aviation (i.e., non-regulated) landing facilities and airports.

Working Group members participating in creating these guidelines are:

- Aircraft Owners & Pilots Association;
- Airport Consultants Council;
- American Association of Airport Executives;
- Experimental Aircraft Association;
- General Aviation Manufacturers Association;
- Helicopter Association International;
- National Air Transportation Association;
- National Association of State Aviation Officials;
- National Business Aviation Association; and,
- United States Parachute Association.

Additionally, individuals representing specific general aviation airports and representatives of various state government aviation agencies fully participated in the working group's activities. Representatives from the Federal Aviation Administration (FAA) and the TSA also participated in the project.

It is the working group's expectation that this document will provide greater consistency for local security requirements involving airport owners, tenants and aircraft operators by providing a list of guidelines.

October 1, 2003

An important concept in developing and implementing these guidelines is avoiding any unfunded mandates to airports, states, general aviation businesses and pilots. Consequently, funding remains a major challenge in addressing many of the security enhancements contemplated by this group. Given the importance of general aviation to the nation's economy, decision-makers at the local, state and federal levels must provide additional resources to GA facilities. In particular, direct federal assistance, changes to the Airport Improvement Program (AIP) and other funding mechanisms merit attention. It is not the Working Group's intent that these security guidelines adversely affect or supplant AIP projects designed to enhance capacity or safety.

The AIP continues to bear a significant portion of the aviation security funding burden and, as those funds are expended primarily for commercial service facility security-related projects, the maintenance and vitality of current general aviation infrastructure dims. As increasingly larger slices of the AIP are used for security costs, many GA facilities are finding themselves unable to compete for and obtain shrinking slices of the pie dedicated to GA. There are currently no dedicated aviation trust funds or other funding sources available for enhancing GA security.

Lacking a comprehensive security risk assessment encompassing all transportation modes, it is important that general aviation not be isolated and required to follow security practices that are beyond those being followed as best practices by other modes of transportation.

Defining General Aviation

General aviation encompasses all civil aviation, except scheduled passenger service and the military. Some basic statistics available from the FAA and from the industry organizations participating in the Working Group demonstrate the breadth and depth of general aviation and its impact on the U.S. economy:

- More than 18,000 landing facilities nationwide serve general aviation, including heliports, lakes and dirt landing strips in remote wilderness areas as well as general aviation airports near urban settings that rival the size and scope of some air carrier airports.
- The more than 219,000 general aviation aircraft in the U.S. are responsible for 77% of all air traffic.
- These aircraft range from one-person "ultralights" and powered parachutes with extremely limited range and payload capabilities to helicopters, seaplanes, antiques, fabric-and-wood biplanes, "homebuilt" experimental airplanes, the ubiquitous four-seat single-engine airplane, twin turboprops, and large and small business jets.
- General aviation accounts for over 637,000 jobs, with nearly \$20 billion in annual earnings. Its direct and indirect economic impact exceeds \$102 billion annually.

October 1, 2003

- There are more than 600,000 certificated pilots in the U.S., most of whom conduct general aviation flight operations.
- General aviation transports approximately 180 million passengers annually in aircraft of all sizes for business and personal reasons.
- An estimated 65% of all general aviation flights are conducted for business and corporate travel.
- Commercial, non-scheduled flights (charters) are also a component of general aviation, with more than 22,000 pilots flying some 14,700 aircraft for this industry segment during 2001 alone.
- General aviation aircraft are used for a wide range of flight operations including personal/family transportation, training, MEDEVAC, transporting medical supplies, emergency services, rescue operations, wildlife surveys, traffic reporting, agricultural aviation and law enforcement.

Because of this wide variety and scope of aircraft and landing locations, any approach to implementing these security guidelines must consider the differing types of various flight operations as well as the size of aircraft involved, among other factors. As one result, a flexible, common-sense approach to general aviation airport security is mandatory if the industry is to retain its economic vitality and prosper.

Government Actions

Since September 11, 2001, the federal government has taken numerous actions related to aviation security. While the terrorist attacks of September 11 were not orchestrated using general aviation aircraft, the federal government nevertheless has taken actions that affect general aviation operators. These federal actions include the following:

Pilots

- **Advanced Screening of Pilot Databases.** Regulations adopted by the FAA and the TSA on January 24, 2003, permit the immediate suspension, revocation or refusal to issue an airmen certificate to anyone that the TSA has determined poses a threat to transportation security. This is based on TSA information as well as that provided by other security agencies.
 - **New Airman Certificate.** In July 2003, the Department of Transportation announced it would begin issuing a new, security-enhanced airman certificate. The difficult-to-counterfeit certificates include a hologram and graphics printed on a plastic card and replace a paper-based document.
 - **Requirement to Carry Photo ID.** An FAA requirement, adopted in October 2002, requires a pilot to carry government-issued photo identification along with the pilot certificate when operating an aircraft.
-

October 1, 2003

- **Restrictions for Foreign Pilots.** There are current federal restrictions on flight training of foreign nationals, including a requirement for background checks for individuals seeking to receive a U.S. pilot certificate on the basis of a foreign pilot certificate. This requirement was put in place in July 2002.
- **Background Checks for Certain Flight Training.** A federal requirement mandates that the U.S. Department of Justice conduct a comprehensive background check for all non-U.S. citizens seeking flight training in aircraft weighing more than 12,500 pounds. Legislation expanding this requirement to include notification to the federal government of all foreign nationals seeking pilot training regardless of aircraft weight has been approved by Congress and is awaiting final action in the Conference Report accompanying the FAA reauthorization legislation (H.R. 2115).

Commercial Operators/Businesses

- **Charter Flight Security Program.** The Twelve-Five and Private Charter rules, which establish new requirements for non-scheduled commercial operators (charters) that provide a level of security equivalent to that of scheduled airlines, became effective April 1, 2003. The following table highlights some of the two programs' various elements:

Private Charter Program Requirements	Twelve-Five Program Requirements
Part 121 and 135 (U.S. aircraft operators) for flights to, from, within, and outside the U.S.	Part 121 and 135 (U.S. aircraft operators) for flights to, from, within, and outside the U.S.
Private charter (passenger) operations only.	Private charter (passenger), scheduled passenger and all-cargo operations.
(1) All aircraft for "sterile" (i.e., loading or unloading in certain areas of a commercial airport) operations. (2) Aircraft weighing 100,300 pounds or more, or 61 or more seats for "non-sterile" operations.	(1) Aircraft weighing 12,500 pounds or more for all-cargo operations. (2) Aircraft weighing 12,500 pounds or more, but less than 100,300 pounds for private charter (passenger) operations.
Passenger identification checks.	Passenger identification checks.
Fingerprint-based CHRC for flight deck crewmembers.	Fingerprint-based CHRC for flight deck crewmembers.
Bomb and hijack notification requirements.	Bomb and hijack notification requirements.
Additional measures protected as Sensitive Security Information.	Additional measures protected as Sensitive Security Information.

Charter flight operations are commonly considered to be part of general aviation, although much more stringent operational and certification requirements are imposed on them than is the case for non-commercial flights.

- **Flight School Security.** In January 2002, the FAA issued a number of recommended actions addressing security for flight schools and those renting aircraft. These recommendations are designed to provide security against the unauthorized use of a flight school or rental aircraft.

October 1, 2003

- **Flight School Security Awareness Training.** Also included in the pending Conference Report accompanying the FAA reauthorization legislation (H.R. 2115) is a requirement that employees be trained in “suspicious circumstances and activities of individuals enrolling or attending” a flight school.

Airports/Airspace

- **Washington DC ADIZ, FRZ and Department of Defense Airspace Restrictions.** Since September 11, the FAA and government officials have imposed airspace restrictions at various locations throughout the U.S. to limit or prohibit aircraft operations in certain areas when intelligence officials report heightened security sensitivity. This includes the Air Defense Identification Zone (ADIZ) around Washington, D.C., the associated Flight Restricted Zone (FRZ) and restrictions that are put into effect when the President travels outside of Washington D.C. These airspace restrictions are patrolled and enforced by U.S. Customs and U.S. military aircraft.
- **Hotline to Report Suspicious Activity.** In December 2002, the TSA implemented a Hotline (1-866-GA-SECURE), which is operated 24/7 by the National Response Center managed by the U.S. Department of Homeland Security that allows anyone to report suspicious activity to a central command structure.
- **Ronald Reagan Washington National Airport.** Ronald Reagan Washington National Airport (DCA) remains closed to all general aviation operations except those few specifically permitted by waiver.
- **Special Flight Rules Area within 15 miles of Washington DC.** Special Federal Aviation Regulation 94 (SFAR 94), implemented on February 19, 2002, prohibits general aviation operations within this 15-mile area unless authorized by the TSA. This limits access at Potomac Airpark, Washington Executive/Hyde Field and College Park Airport (referred to as the “DC-3”) to only cleared and vetted pilots operating in compliance with specific flight planning and ATC procedures.
- **Limits on Flights Over Stadiums.** A pre-existing Notice to Airman (NOTAM) was updated on March 6, 2003, due to enactment of P.L. 108-7 that limits aircraft operations in the airspace over major sporting events. Commercial operators with a need to fly within 3 nautical miles and below 3,000 feet of an event stadium must apply for a waiver through the TSA and must complete a pilot vetting process to obtain that waiver. Banner towing operations are prevented from flying over major sporting events (college football, professional baseball and football, NASCAR and other specifically identified events). Other restrictions may be applied on a case-by-case basis when deemed appropriate by federal authorities, e.g., the 2002 Winter Olympics.
- **No Flights Over Nuclear Facilities.** On February 26, 2003, a pre-existing NOTAM advising pilots not to circle or loiter over nuclear facilities was strengthened to reinforce the need for pilots to avoid these facilities altogether.

October 1, 2003

Industry Actions

Individual general aviation organizations have taken pro-active steps to increase security and security awareness. Aviation, while substantial in economic impact and number of operations, is relatively small when compared to other transportation modes such as maritime, rail or highways. As such, general aviation operators are keenly aware of and willing to individually enhance the security of their operations without government regulation. Given the ease and frequency of intrastate movement, combined with the wide variety of operations, measures taken by individual operators are more comprehensive than regulation at the state or federal level.

Following is a brief description of some, but not all, of the security-based actions and recommendations of these organizations in the last two years.

- **Aircraft Owners and Pilots Association.** The Aircraft Owners and Pilots Association (AOPA) developed a nationwide aviation watch system (Airport Watch) using the nation's 650,000 pilots that is supported by the TSA centralized toll-free hotline and system for reporting and acting on information provided by general aviation pilots and other individuals at airports. *The Airport Watch Program* includes warning signs for airports, informational literature, and a training videotape to educate pilots and airport employees as to how the security of their airports and aircraft can be enhanced.
- **Airports & Airport Tenants.** Many airports and individual airport tenants have already implemented security enhancements in addition to the aforementioned *Airport Watch Program*. Such initiatives have included but are not limited to installing alarm systems, controlling access, monitoring and improving gates, fencing and lighting. Some airports are also experimenting with new technologies in security monitoring, surveillance and access control technologies, including WiFi and sophisticated target acquisition software programs.
- **American Association of Airport Executives.** The American Association of Airport Executives (AAAE) "General Aviation Airport Security Task Force" delivered a set of recommendations to the TSA in June 2002. The eight recommendations made by AAAE were developed by establishing categories of airports based on runway length and number of based aircraft. Recommendations also included securing aircraft, establishing a threat communication system, developing a new pilot license, securing aircraft, and expanding the FAA contract tower program.
- **Experimental Aircraft Association.** The Experimental Aircraft Association (EAA) mobilized its network of nearly 1000 chapters nationwide to improve security at many of the nation's airports through increased knowledge and vigilance. To support this effort, *Airport Watch* videotapes and other educational materials concerning security practices and airspace restrictions were distributed nationwide. In addition, Notices to Airmen (NOTAMs), often employing graphic depictions, are provided near-real-time to pilots via the association's Web site and direct e-mail, warning of security sensitive areas and

October 1, 2003

airport closures. EAA has led the development of new Sport Pilot and Light Sport Aircraft regulations which, in part, will have the positive security impact of registering with the FAA an estimated ten to fifteen thousand previously unregistered ultralight training aircraft and certificating a similar number of ultralight pilots and instructors that heretofore had not been part of the FAA certification process.

- **General Aviation Coalition.** In December 2001, the GAC issued a series of 12 recommendations for general aviation security. The government and the general aviation community have implemented many of these. In addition, the TSA conducts regular meetings with the GAC to address general aviation security issues.
- **General Aviation Manufacturers Association.** The General Aviation Manufacturers Association (GAMA), in conjunction with the U.S. Department of the Treasury, is working to help aircraft sellers identify unusual financial transactions that could indicate attempts to launder money via the purchase of aircraft, or otherwise suspicious customer behavior. The publication entitled "Guidelines for Establishing Anti-Money Laundering Procedures and Practices Related to the Purchase of General Aviation Aircraft" was developed in consultation with manufacturers, aviation-finance companies, used aircraft brokers and fractional ownership companies.
- **National Agricultural Aircraft Association.** The National Agricultural Aircraft Association (NAAA) has produced an educational program called the Professional Aerial Applicators Support System (PAASS) that includes a new educational portion every year, specifically addressing security of aerial application operations. The PAASS program annually reaches roughly 2,000 people involved in aerial application. It is presented at state and regional agricultural aviation association meetings throughout the country. In addition, NAAA members have undergone several industry-wide FBI background investigations since 9/11/01.
- **National Air Transportation Association.** On September 24, 2001, the National Air Transportation Association (NATA) issued a series of recommended security procedures for all aviation businesses through its Business Aviation Security Task Force. The recommendations focused on immediate steps that should be taken, plus longer-term actions. Examples included signage, appointing a single manager responsible for security at all locations, developing a "security mission statement," methods to verify identification, seeking local law enforcement assistance to develop a security plan and a host of others, including an advisory poster that was created and distributed free to all NATA members.
- **National Association of Flight Instructors.** The National Association of Flight Instructors (NAFI), an affiliate of EAA, has developed a series of security recommendations and best practices for flight schools and flight instructors that have been distributed widely throughout the flight training community. Currently, NAFI is working in cooperation with the TSA to develop training materials and distribution methods in support of the proposed flight school security awareness training

October 1, 2003

requirements contained in the pending Conference Report accompanying the FAA reauthorization legislation (H.R. 2115).

- **National Association of State Aviation Officials.** In December 2002, the National Association of State Aviation Officials (NASAO) submitted to federal and state authorities a document outlining general aviation security recommendations. This included securing unattended aircraft, developing a security plan, and establishing a means to report suspicious activity. In addition, airports should establish a public awareness campaign; perform regular inspection of airport property and control movement of persons and vehicles in the aircraft operating area. The state aviation officials suggested federal authorities implement a new pilot ID, establish a means to verify the identity of persons requesting flight lessons with a government watch list, implement a process for categorizing airports, and ensure adequate federal funding for airport security needs.
- **National Business Aviation Association.** The TSA launched a pilot project in cooperation with the National Business Aviation Association (NBAA) at Teterboro Airport (KTEB) in New Jersey. This has been expanded by the TSA to include Part 91 operators based at Morristown, New Jersey, (KMMU) and White Plains, New York, (KHPN). This initiative is proceeding as a “proof-of-concept” validating an NBAA-proposed security protocol for Part 91 operators who can apply for a TSA Access Certificate (TSAAC). Once issued, the TSAAC allows operators to operate internationally without the need for a waiver. The TSA is also considering granting access for TSAAC holders to designated TFRs.
- **United States Parachute Association.** USPA disseminated detailed security recommendations to its 219 skydiving clubs and centers across the U.S., most of them based on general aviation airports. Skydive operators and their customers are often on airports during days and hours when others are not, and can enhance any airport watch program. Other recommendations were aimed at ensuring security of jump aircraft during operations as well as periods when aircraft are idle.

Methodology

Members of the Working Group met six times throughout the summer of 2003 and engaged in extensive discussions to review numerous general aviation airport security recommendations, including those “industry best practices” mentioned above. In each instance, Working Group members collectively evaluated each recommendation for its appropriateness and its effect on enhancing general aviation airport security. One result of these efforts is the guidelines included herein. Their primary purpose is to help prevent the unauthorized use of a general aviation aircraft in an act of terrorism against the United States, an event which has never before occurred.

October 1, 2003

The Working Group's recommendations are focused on listing those guidelines the federal government should recommend to airport managers and operators to enhance the security of their facility.

The Working Group focused on no-cost or low-cost guidelines, in large measure due to the lack of federally appropriated funds for general aviation security and the resultant adverse economic impact that would otherwise be imposed on general aviation airports. Any unfunded mandates will have a significant impact on communities that own general aviation airports, GA airport operators, GA tenants and users alike. In particular, unfunded mandates will have the most impact where the relationship between cost and benefit remain poorly understood.

Implementation

Managers and operators of general aviation airports are encouraged to use the recommended guidelines in this report to enhance the security of their respective facilities. When considering the scope and breadth of these recommendations, it may be helpful to develop a written security protocol. Such a protocol should minimally consist of, but not be limited to, airport and local law enforcement contact information, including alternates when available. More extensive protocols may call for, but not be limited to, emergency locator maps, entrance locations and response procedures.

Each written general aviation security protocol should include reference to and be coordinated with appropriate local response plans as prepared for the specific region in which the landing facility is located. The protocol should emphasize such critical elements as awareness, prevention, preparation, response and recovery.

Intrinsic in these recommended guidelines is the concept that each general aviation airport is unique. As a result, the Working Group went to great lengths to make these recommendations relevant to each airport and landing facility, whether it is adjacent to a major metropolitan area or situated in a remote area.

As one result, these recommendations are both broad in their scope and generic in their application. Each and every general aviation airport and landing facility operator throughout the U.S. may use them to evaluate that facility's physical security, procedures, infrastructure and resources.

October 1, 2003

Recommendations

The following specific recommendations were selected in assisting the local aviation community in the development of a tiered but flexible security plan given available resources, alert levels and potential threats.

Personnel

Passengers

- Prior to boarding, the Pilot In Command should ensure that the identity of all occupants is verified, all occupants are aboard at the invitation of the owner/operator, and that all baggage and cargo is known to the occupants.

Pilots

- Pilots must be able to provide government-issued photo identification.

Student Pilots

- Control aircraft ignition keys so that the student cannot start the aircraft until the instructor is ready for the flight to begin or
 - Limit student pilot access to aircraft keys until the student pilot has reached an appropriate point in the training curriculum; or,
 - Consider having any student pilot check in with a specific employee (i.e. dispatcher, aircraft scheduler, flight instructor, or other "management" official) before being allowed access to parked aircraft; or,
 - Have the student sign or initial a form and not receive keys until an instructor or other "management official" also signs or initials; or,
 - When available, use a different ignition key from the door lock key. The instructor would provide the ignition key when he or she arrives at the aircraft.

Flight Schools and Aircraft Renters

- The identity of an individual renting an aircraft should be verified by checking a government-issued photo ID as well as the airman certificate and current medical certificate (if necessary for that operation).

October 1, 2003

- In addition to any aircraft-specific operational and training requirements, a first-time rental customer should be familiarized with local airport operations, including security procedures used at the facility.
- Operators renting aircraft should be aware of suspicious activities and report to appropriate officials individuals who inquire about aircraft rental without possessing the necessary knowledge or certifications to operate such an aircraft.

Transient Pilots

- Sign-in/sign-out procedures for all transient operators identifying their parked aircraft.

Aircraft

Securing Aircraft

- Pilots should make it as difficult as possible for an unauthorized person to gain access to their airplane. This would include using existing mechanisms such as door locks, keyed ignitions, hangaring the aircraft or using an auxiliary lock to further protect aircraft from unauthorized use. Commercially available options for auxiliary locks include locks for propellers, throttle, and prop controls, and tie-downs. Locking hangar doors and aircraft doors to prevent unauthorized access or tampering with the aircraft is important.

Airports/Facilities

Airport Vehicle Access

- Consider reasonable vehicle access control to facilities and ramps, which may include signage, fencing, gates or positive control techniques. This may include restricting access to the airside to as few locations as possible, balancing the need for authorized access with access control.
 - Where there is access control, periodically review access authorization – including codes, cards and locks – to vehicular and pedestrian gates leading to airside.

Lighting

- Consider installing effective outdoor area lighting to help improve the security of (a) aircraft parking and hangar areas; (b) fuel storage areas, (c) airport access points; and other appropriate areas. Proximity sensors should be considered.

October 1, 2003

Hangars

- Secure hangar/personnel doors when unattended.

Signage

- It is recommended that airports post appropriate signage. Wording may include – but is not limited to – warnings against trespassing, unauthorized use of aircraft and tampering with aircraft, as well as reporting of suspicious activity. Signage should include phone numbers of the nearest responding law enforcement agency, 9-1-1, or TSA's 1-866-GA-SECURE, whichever is appropriate.

Surveillance

Airport Community Watch Program

- Establish an Airport Watch Program (These recommendations are not all inclusive. Additional measures that are specific to your airport should be added as appropriate.)
 - Utilize AOPA Airport Watch Program; and/or
 - Develop similar watch program to include the following items, if appropriate:
 - ✓ Coordinate locally with airport officials, pilots, businesses and/or other airport users.
 - ✓ Hold periodic meetings with the airport community.
 - ✓ Develop and circulate reporting procedures to all who have a regular presence on the airport.
 - ✓ Encourage proactive participation in aircraft and facility security and heightened awareness measures. This should encourage airport and line staff to 'query' unknowns on ramps, near aircraft, etc.
 - ✓ Post signs promoting the program, warning that the airport is watched. Include appropriate emergency phone numbers on the sign.
 - ✓ Provide training to all involved for recognizing suspicious activity and appropriate response tactics.
 - This could include the use of a video or other media for training. The following are some recommended training topics:
 - Transient aircraft with unusual or unauthorized modifications.

October 1, 2003

- Persons loitering for extended periods in the vicinity of parked aircraft, in pilot lounges, or other inappropriate areas.
 - Pilots who appear to be under the control of another person.
 - Persons wishing to rent aircraft without presenting proper credentials or identification.
 - Persons who present apparently valid credentials but who do not display a corresponding level of aviation knowledge.
 - Any pilot who makes threats or statements inconsistent with normal uses of aircraft.
 - Events or circumstances that do not fit the pattern of lawful, normal activity at an airport.
- ✓ Utilize local law enforcement for airport security community education.
 - ✓ It is recommended that airports post appropriate signage. Wording may include – but is not limited to – warnings against trespassing; unauthorized use of aircraft; and tampering with aircraft, as well as reporting suspicious activity. Signage should include phone numbers of the nearest responding law enforcement agency, 9-1-1 or TSA’s 1-866-GA-SECURE whichever is appropriate.
- Encourage employers to make their staff aware of the airport watch programs.

Law Enforcement Officer Support

- Develop procedures to have security patrols for ramp and aircraft hangar and parking areas. Special considerations should be made during periods of heightened security.
- Airport operators should communicate and educate local law enforcement agencies on security procedures at the airport. This could include:
 - What does a pilot license look like;
 - Who is authorized to drive on the ramp;
 - How do you get airport access (who has key);and
 - What are “normal” operations.

October 1, 2003

Security Plans & Communications

Security Plan

- Create an emergency locator map. Identify gates, hydrants, emergency shelters, buildings and hazardous materials sites on a grid map. Provide fire and law enforcement with a copy of the map. Also, establish a procedure for handling bomb threats and suspect aircraft.

Threat Communication System

- Develop a tiered comprehensive local phone and contact list and distribute on a need-to-know basis. Include the following 24-hour phone numbers on the contact list:
 - Airport Director
 - Point of Contact or Airport Security Coordinator
 - Local Police or County Sheriff Department (List all responding LEO Agencies)
 - County/City Emergency Manager
 - State Police
 - Fire Department
 - State Office of Public Security
 - FBI, FAA or TSA
 - Any other appropriate organization

Where possible, establish radio communication capabilities with local law enforcement.

- The TSA and industry shall post these best practices on their respective Web sites and related information about securing aircraft and airport facilities. Existing security courses available from industry should be identified, including those from AAAE, AOPA, EAA, and NATA.
- Communicate and educate all new security policies and procedures when issued.
- Conduct regular meetings with airport tenants and the flying public to discuss the security issues and challenges.
- Have a qualified, single Point of Contact (POC) for disseminating security information.

October 1, 2003

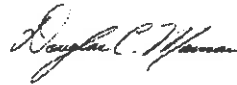
Specialty Operations

Agricultural Aircraft Operations

- It is recommended that each owner/operator of agricultural aircraft take appropriate steps to secure the aircraft when unattended. Examples of existing mechanisms include throttle and control locks, propeller locks and hidden ignition switches. When storing aircraft, it is recommended that aircraft be stored in hangars with steel doors that are locked with electronic security systems. When hangars are not available for storage, it is recommended that heavy equipment be parked in the front and back of agricultural aircraft when not in use.



Andy Cebula
Senior VP for Government and Technical Affairs
Aircraft Owners & Pilots Association



Douglas C. Macnair
Vice President, Government Relations
Experimental Aircraft Association



J. Leonard Wood
Airport Consultants Council



Ronald L. Swanda
Vice President of Operations
General Aviation Manufacturers Association



Rebecca Khamneipur
Senior Director, Transportation Security Policy
American Association of Airport Executives



Richard M. Wright, Jr.
Manager of Administrative Services
Helicopter Association International

Report Of The Aviation Security Advisory Committee Working Group On General Aviation Airports
Security


October 1, 2003



Joseph E. Burnside
Vice President
National Air Transportation Association



Henry M. Ogrodzinski
President and CEO
National Association of State Aviation Officials



Robert P. Blouin
Senior Vice President, Operations
National Business Aviation Association



Ed Scott
Director of Government Relations
U.S. Parachute Association

APPENDIX E

AOPA's Airport Watch



SIMCOM customers

Aircraft Owners and Pilots Association

Contents

What's New ▾

Join/Renew ▾

Aviation Classifieds ▾

Links

Contact Us

Search

Advanced search

PUBLIC SECTION

AOPA Home

About »

AOPA »

Advocacy »

AOPA Magazines »

Member Products »

Air Safety Foundation »

President's Page »

Learn to Fly »

Calendar of Events »

MEMBERS SECTION

My AOPA »

Members Home

Weather »

Flight

Planning

Airport Directory »

A/C Valuation Services

Medical »

Info Resources/FAQs »

Messaging/Chat



What Is AOPA's Airport Watch?

- Why we need Airport Watch
- Be part of AOPA Airport Watch. It's easy!
- Report what you find unusual
- It's your home field - cover your entire neighborhood

- Security begins with your own airplane
- AOPA Airport Watch wants you
- Are you ready to do your share
- **Security checklist**



America's pilots are banding together protect our airport:

Participate with your fellow in the safekeeping of general aviation's neighborhood home airports.

See potential criminal activity at your airport? call 1-866-GA-SECURE

Why we need Airport Watch

Pick up any newspaper and you know why we need an airport watch. General aviation is under suspicion as a potential launch point for terrorist activity. After the events of September 11, 2001, the people in your community may have a different view of airplanes and their potential use as weapons. You may even share that concern. The world changed radically that terrible day, and it is incumbent on us - the people who depend on

AOPA Online - What Is AOPA's Airport Watch?

general aviation aircraft for our livelihood, our recreation, our personal transportation - to do our share to make sure that our airports are safe.

Every pilot is part of the larger aviation community. For pilots, our airports are our communities and we need to protect them just like we watch our own homes and neighborhoods. Pilots are the first to know that someone doesn't belong on the airport or that some activity at the airport is outside normal routines. At general aviation airports, the cost of implementing security programs that might include complete fencing of the airport's perimeter are, for the most part, cost prohibitive.

But, with more than 600,000 pilots based at virtually every general aviation airport in the United States, AOPA and our members have a tremendous opportunity to make a difference in security at GA airports.

There is no doubt that the federal government could not afford, nor is it necessary for them to regulate those airports. That's why AOPA supports 1 866-GA-SECURE. It's the number to call when you see something suspicious at an airport.

In this post-attack atmosphere, we can no longer say, "That could never happen." We don't know what can happen and what can't - even at a quiet little airport. While unlikely, the potential remains for general aviation airplanes to be used by terrorists. This unlikely possibility brings with it the potential for security officials to impose restrictions on airport access and use. We can lessen that need by protecting our own aviation neighborhoods.

Show your community that pilots are keeping watch at their local airports. Be ready to call the National Response Center at 1-866-GA-SECURE

Be part of AOPA's Airport Watch. It's easy!

You just need eyes and ears!

Police departments will tell you that the best protection your home can have is an alert neighbor. AOPA's Airport Watch operates just like a neighborhood watch. The people on a neighborhood watch know their neighbors' habits, who is on vacation, whose car belongs where, and they are able to spot trouble, sometimes before it happens. AOPA is bringing the same concept to Airport Watch. We want you to heighten your attention at the airport - get to know your fellow hangar tenants, pilots, and aircraft owners.



Being part of AOPA's Airport Watch doesn't take extra time. All you have to do is go about your business at the airport - whether it's flying, hangar flying, performing maintenance, or just socializing. You don't have to write reports or attend lengthy meetings. Just follow these guidelines and be prepared to call 1-866-GA-SECURE if you see any activity that does not seem right to

AOPA Online - What Is AOPA's Airport Watch?

see any activity that does not seem right to you.

Here are some ways pilots can show their communities that pilots are responsible citizens who are concerned about security at our airports. Remember, these tips work best with frequent visits to your airport!

- **Have your ID ready.** Always carry a government-issued photo ID for yourself. Even though you know your passengers, insist that they also arrive with government-issued picture identification in case of challenge by security or airport personnel. It also makes sense to carry your pilot certificate with you, even if you're not flying that day. Most pilots carry these in their wallets, but the combination of a photo ID and a pilot certificate is now required by the FAA.
- **Be cooperative.** We want the community to know that we are willing to comply with added security measures. You may have flown out of the same airport for 20 years and think "everybody knows me," but the brand-new security guard doesn't. Make it easy for them to do their job, and be thankful that they're doing it well.
- **Share information.** Supply your airport operator or FBO with photo of pilots authorized to use your airplane so that new or infrequent users won't be mistaken for an unauthorized lawbreaker. If someone else is going to fly your aircraft, inform your FBO by telephone. Let ramp staff know anytime your plane is RON so they know it's not missing without reason; inform them when the airplane is to be down or shouldn't be going anywhere, so they can challenge any movement of your airplane during the period of inactivity.
- **Get to know your airport community.** Introduce yourself to airport neighbors and become familiar with the aircraft these neighbors fly. Not only will you meet and interact with new people and new airplanes, but also you'll be better prepared to notice new airplanes and new faces at your airport.
- **Greet strangers.** Introduce yourself to new faces at your airport - particularly new flight students and visitors to your home field and transient pilots you meet. At once, you can resolve many questions about these folks and help give your home airport a reputation as a friendly place to fly.
- **Stand united.** Organize (or help organize) a series of meetings at the airport to discuss security issues, any changes or new rules, and to generally get to know your airport neighbors while sharing in the effort to protect your community. If such meetings already exist, attend. Believe that "it can happen here" and don't wait for the other guy to take charge.
- **Have your tools handy.** Bring your cell phone to the airport - and make sure it's charged. Have a pen and paper close by in case you have to write down N numbers or descriptions. Consider having an inexpensive camera - even a disposable one - at the ready to photograph what you see that is suspicious.
- **Spread the word.** Talk about AOPA's Airport Watch. Let people know that general aviation pilots take security at our airports seriously, that we voluntarily act to be on the alert for what is happening at our airports. You'll also reinforce the message that the general aviation community takes care of itself without the need for increased and possibly burdensome government regulations.
- **Be prepared for the long haul.** Keep the effort going. Help sustain these and other security efforts once they're started. The new reality of operating aircraft post 9/11 is not a drill and it's not a flash in the

AOPA Online - What Is AOPA's Airport Watch?

pan.

Momentum must be sustained in the long term, both for the safety and security of our airplanes and airports, as well as for our long-term protection from the imposition of rules that impinge on our freedom to fly.

Report what you find unusual!

First call 1-866-GA-SECURE or 911 in an emergency. Then share the information with airport management or staff.

NEVER approach someone you fear may be about to commit an illegal act or crime with an airplane. Make some notes, such as the person's appearance, clothing, car license plate, type of aircraft, and N number. Take a picture, but keep your distance if the situation seems hostile. If you can't safely contact the closest authorities or the airport management without exposing yourself to risk, leave the field or go to your car and talk on your cell phone. It could be your best weapon in fighting airport crime.



Provide details. Be specific in details whenever you report something amiss to authorities. Generalized concerns (e.g., "That guy looked shifty to me...") may not carry the appropriate sense of urgency.

Details carry weight:

"I'm at the Anytown Municipal Airport and just saw [something dangerous] loaded into a tan-and-orange plane with the N number N123. The pilot seems to be intimidated by his passengers; the passengers are keeping out of sight. I think something bad is about to happen." Pay attention to height, weight, clothing, or other identifiable traits.

Never hesitate to call 1-866-GA-SECURE!

If danger is imminent, call 911.

We can never be too sure of our safety!

It's your home field - cover your entire neighborhood!

Some situations require special attention. Not every one of your home neighbors is the same, so here are some tips for handling special situations:

For CFIs with primary student pilots:

Control non-solo students' access to the ignition key until dual is to begin. The CFI might unlock the airplane for preflight and keep the ignition key; install an ignition switch keyed differently than airframe keys; or allow access to the ignition key but install a throttle lock for which the CFI retains the key. Depending on the environment, it might be useful to assign a special check-on for students (soloed and presolo) - particularly

AOPA Online - What Is AOPA's Airport Watch?

younger students.



For FBO rental desks:

Create a check-in desk and procedure where keys to based and transient aircraft (or hangar keys for based planes) are kept for checkout to pilots and owners with preauthorization on file. Encourage owners of rental or loaned airplanes to provide advance photo records of those authorized to rent or use their aircraft. Insist on photo ID for pilots not personally known to the staff. It's for their good as well as the public's. Establish uniform "duress procedures."

For ag applicators:

Provide airport neighbors and management with a list of all people with authorized access to your equipment - consider including a photo of those people. Increase the strength of locks on chemical storage areas and add multiple auxiliary locks to your applicator aircraft.

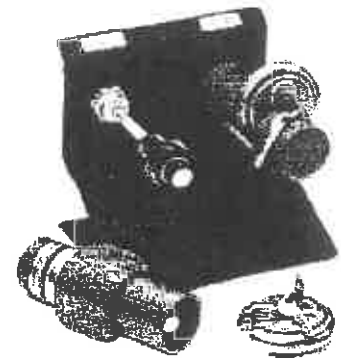
Remember: Crime happens because of opportunity. To protect yourself and your airport, make access difficult. Criminals won't want to hang around an airport full of people who are alert and aware of their activities. Exposure is not within the comfort zone of a criminal.

It's up to all of us who fly to keep flying safe, to keep our airports free of individuals who would do us harm, and to welcome those who truly want to share our freedom to fly.

Protect that freedom to fly - join AOPA's Airport Watch program today!

Security begins with your own airplane

Charity may begin at home, but so does security. People seldom forget to lock their homes; cars are locked less frequently. But too often pilots neglect to lock the doors of their aircraft. "It's always hangared;" "It's too easy to break into;" "I'm just running out to get a sandwich;" are all excuses for poor security.



Crime happens because of opportunity. Don't ever make it easy for anyone! Lock your airplane's doors, regardless of whether your airplane is hangared or tied outside - always!



For added security, consider using an auxiliary lock to further protect your aircraft from unauthorized use. Options available include several fine locks for propellers, throttle, and prop controls. Pilot supply catalogs have a wide range of products to deter

AOPA Online - What Is AOPA's Airport Watch?



tampering and theft of your aircraft.

Then take home all your keys - to the airplane, hangar, and auxiliary locks. You might want to consider whether you keep your airplane key on the same keychain as your hangar key. Make it as difficult as possible for someone to gain access to your airplane.

Together we can make general aviation the least attractive option available to the terrorist or other criminal!

AOPA Airport Watch wants you

America's pilots should be on the frontlines of monitoring what goes on at our airports. When we band together, we become a powerful network of watchdogs for what is happening at our airports. It's just common sense: We spend time at the airport, we know the people, we know the airplanes.

It's self-defeating for us as general aviation pilots to dig in our heels and act as if our community and government officials should simply understand and accept what we know about aircraft, pilots, and all the regulations we live by. It's a different world, and we must adapt to it. We must step up to today's challenge. We must do our share to guard against criminal activity at our airports.

AOPA's Airport Watch program will protect our homes and neighbors by guarding our aircraft and the airports we use. When you call 1-866-GA-SECURE, you will act as part of a community-wide general aviation effort to protect our aircraft, our airports, and our aviation communities.

We can protect our freedom to fly by simply exercising our freedom to fly, by visiting our airports often, and by joining general aviation's own airport community safety program, the AOPA's Airport Watch. Begin your participation now!

America's pilots banding together will make a difference.

Are you ready to do your share?

Your participation at your local airport will make this program a success. Now you don't have to wonder what you can do to ensure you will be able to enjoy the freedom of flight. Without your help, others - who don't love airplanes like we do - will impose their own security program on our community!

Through the AOPA Airport Watch Program, we have the power to reduce or even eliminate the perception that private airplanes pose a significant threat to the public. Protect our flying community and our freedom to fly while protecting our nonflying friends and neighbors by protecting your airplane and airport like you do your home and neighborhood!

Use your eyes and ears to keep our

airports safe

Here's what to look for:

- Pilots who appear under the control of someone else.
- Anyone trying to access an aircraft through force - without keys, using a crowbar or screwdriver.
- Anyone who seems unfamiliar with aviation procedures trying to check out an airplane.
- Anyone who misuses aviation lingo - or seems too eager to use all the lingo
- People or groups who seem determined to keep to themselves.
- Any members of your airport neighborhood who work to avoid contact with you or other airport tenants.
- Anyone who appears to be just loitering, with no specific reason for being there.
- Any out-of-the-ordinary videotaping of aircraft or hangars.
- Aircraft with unusual or obviously unauthorized modifications.
- Dangerous cargo or loads - explosives, chemicals, openly displayed weapons - being loaded into an airplane.
- Anything that strikes you as wrong - listen to your gut instinct, and then follow through.
- Pay special attention to height, weight, and the individual's clothing or other identifiable traits.

*Use your common sense.
Not all these items indicate
terrorist activity.*

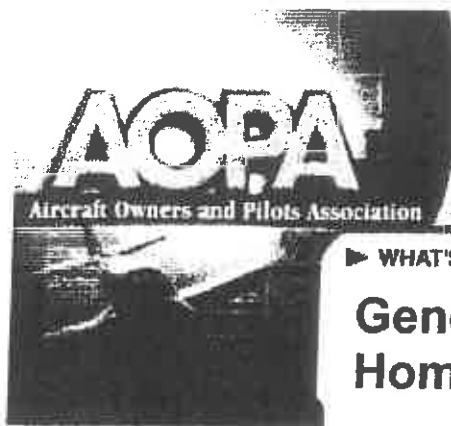
When in doubt, check it out!
Check with airport staff or call
the National Response Center
at 1-866-GA-SECURE!

[Top](#) [Printer Friendly Version](#)

Public section: [Home](#) | [Table of contents](#) | [About AOPA](#) | [Join or renew](#) | [What's new](#) | [Advocacy](#) | [AOPA Pilot magazine](#) | [Certified products](#) | [Air Safety Foundation](#) | [President's page](#) | [Learn to fly](#) | [Web links](#) | [Classified ads](#) | [Search](#)

Members section: [Register for access](#) | [Members home](#) | [Weather](#) | [Flight planning](#) | [Airport directory](#) | [Aircraft valuation service](#) | [Medical Information resources](#) | [Messaging/chat](#) | [Member profile](#)

Special access: [Airport Support Network](#) | [Press Center](#)



NEW! Introducing the PMA7000MS-CD **NEW!**
The extremely versatile Audio Panel
with remote mounted Compact Disc Player



Aircraft Owners and Pilots Association

[Contents](#) [What's New](#) [Join/Renew](#) [Aviation Classifieds](#) [Links](#) [Contact Us](#)

▶ **WHAT'S NEW**

General Aviation and Homeland Security

A security brief by the Aircraft Owners and Pilots Association



Search

Advanced search

Sponsored by



PUBLIC SECTION

[AOPA Home](#)

About

[AOPA](#) »

[Advocacy](#) »

[AOPA Magazines](#) »

[Member Products](#) »

[Air Safety Foundation](#) »

[President's Page](#) »

[Learn to Fly](#) »

[Calendar of Events](#) »

MEMBERS SECTION

[My AOPA](#) »

[Members Home](#)

[Weather](#) »

Flight

[Planning](#)

[Airport Directory](#) »

[A/C Valuation Services](#)

[Medical](#) »

[Info Resources/FAQs](#) »

[Messaging/Chat](#)

- **General aviation aircraft do not pose a significant terrorist threat to the U.S.**

In fact, there has been no terrorist attack anywhere in the world using a general aviation aircraft.

- **The U.S. government has determined that GA is not a significant threat**

Since the September 11 attacks, no segment of aviation has been under more scrutiny than general aviation. After grounding all aviation in September 2001, the federal government then incrementally restored flight operations after careful security review. The White House Office of Homeland Security (predecessor of today's cabinet-level Homeland Security Department), the Transportation Security Administration (TSA), the Department of Defense, the National Security Council, the Secret Service, the FBI, the Department of Transportation, the FAA and other agencies have specifically examined general aviation flight operations in all parts of the nation and have sanctioned continued GA flight under current regulations.

- **The GA industry has voluntarily taken positive steps to enhance security**

AOPA, in cooperation with the Transportation Security Administrator has implemented Airport Watch enlisting the help of the more than 550,000 general aviation pilots to watch for and report suspicious activities at the nation's airports. Modeled after neighborhood watch programs, AOPA's Airport Watch includes a national, toll-free hotline (866-GA-SECURE), staffed by the federal government's National Response Center. The Airport Watch brochure was mailed to some 389,000 AOPA members in December 2002, and TSA sent it to the remainder of the pilot population. A video is also available to pilots' groups. The video contains dramatizations of some of the situations pilots ought to be on the lookout for.

AOPA and other industry organizations offered a 12-point plan to enhance security in December 2001. The government eventually adopted most of the proposals.

AOPA Online - General Aviation and Homeland Security

FAA used the industry recommendations to issue an FAA Order to its Flight Standards District Offices to enhance flight school and airport business (FBO) security.

AOPA petitioned the FAA in February 2002 to require a government-issued photo ID to be carried with a pilot's certificate (license). Congressional committees, key members of Congress, and the Transportation Security Administration endorsed that petition. In October 2002, FAA made a rule change to require the photo ID to better identify legitimate pilots. Then in July 2003, the Department of Transportation announced it would begin issuing a new, difficult-to-counterfeit airman certificate that includes a hologram on a plastic card. (AOPA has for many years asked for the pilot's photo to be on the pilot certificate.)

The General Aviation Manufacturers Association has worked with the U.S. Treasury Department to develop and implement new guidelines on aircraft financial transactions, intended to flag suspicious transactions (e.g., all-cash transactions, third party payments, ambiguous customer identity).

- **General aviation aircraft are incapable of causing significant damage**

More than 70% of the GA fleet are small, single-engine aircraft with six or fewer seats.

The typical GA aircraft (Cessna 172 and similar) weighs less than a Honda Civic and carries even less cargo.

The majority of GA aircraft have less than 1% of the mass of a large airliner. (A fully loaded Cessna 172 weighs approximately 2,400 pounds and carries 56 gallons of fuel. A Boeing 767 can weigh more than 400,000 pounds and carry some 25,000 gallons of fuel.)

The suicide crash of a Cessna into a Tampa office building demonstrates the ineffectiveness of a GA aircraft as a terrorist weapon.

- **GA aircraft are not a threat to nuclear power facilities**

A report by an internationally recognized nuclear security and safety expert concluded that a small aircraft could not cause a release of radiation from a nuclear facility.

- **Small airports are secure by their nature**

A general aviation airport is a small neighborhood. Most people on the airport know each other; suspicious activities are noticed. Since September 11, pilots and others at the airport have stepped up their vigilance, and report their suspicions to authorities. GA pilots are proactively improving security by participating in AOPA's Airport Watch program (see below).

General aviation airports have taken voluntary steps to enhance security. An AOPA survey of airports across the nation found that every one had taken action appropriate to the facility, including the implementation of ID checks, improved fencing, stationing of law enforcement personnel on the field. etc.

- **Hijackers are not likely to gain access to a GA aircraft**
General aviation aircraft are used for personal and business transportation, just like an automobile. Unlike a commercial carrier, the pilot knows the passengers and what they are carrying. Personal knowledge is the most effective security.

- **GA aircraft are not easily stolen**
An aircraft is a high-value item. Even a simple, 30-year-old aircraft can be worth \$40,000 or more. Owners take reasonable precautions to protect that investment. Historically, only about a dozen general aviation aircraft a year are stolen.

The number of GA aircraft stolen is down sharply since the general aviation community has taken steps to enhance security. In 2002, 11 GA aircraft, mostly single engine piston aircraft, were stolen. Through August 2003, only three GA aircraft have been stolen, two single engine and one medium twin engine.

- **The U.S. government has acted to deny pilots' certificates to possible terrorists**
Revocation of pilot certificates — *In January 2003, the FAA issued a rule stating that if the TSA determines that a pilot poses a national security threat, it can direct the FAA to revoke that pilot's certificate. (While AOPA supports the intent of this regulation, the association believes the appeals process in the current regulation is flawed and denies due process to accused pilots. AOPA backs pending legislation that would correct the flaw.)*

Restrictions for foreign pilots — *Since July 2002, federal restrictions on flight training of foreign nationals include a requirement for background checks for individuals seeking to receive a U.S. pilot certificate on the basis of a foreign pilot certificate.*

Background checks for certain flight training — *A federal requirement mandates that the U.S. Department of Justice conduct a comprehensive background check for all non-U.S. citizens seeking flight training in larger aircraft weighing more than 12,500 pounds (generally turboprops or jets with more than eight seats). Legislation expanding this requirement to include notification to the federal government of all foreign nationals seeking pilot training regardless of aircraft weight is pending.*

- **The U.S. government has taken additional steps to enhance aviation security**
Commercial Operators/Businesses —

Charter flight security program — *The federal government has established security requirements for aircraft charter operations - especially those using larger, heavier aircraft - that are more in line with airline security measures.*

Flight school security — *In January 2002, the FAA issued a number of recommended actions addressing security for flight schools and those renting aircraft.*

Flight school security awareness training — Pending federal legislation includes a requirement that flight school employees be trained to recognize "suspicious circumstances and activities of individuals enrolling or attending" a flight school.

Airports/Airspace —

Washington D.C. ADIZ, FRZ, and Dept. of Defense airspace restrictions — Since September 11, the FAA and homeland security officials have imposed airspace restrictions at various locations throughout the U.S. when intelligence indicates a heightened security threat. These include the Air Defense Identification Zone (ADIZ) and associated Flight Restricted Zone (FRZ) around Washington, D.C., and temporary flight restrictions that are put into effect when the President travels outside Washington, D.C. These restricted airspace areas are patrolled and enforced by U.S. Customs and military aircraft.

Stadium overflights — during an event at a stadium, aircraft operations within 3 nautical miles of and less than 3,000 feet above the venue are restricted, unless cleared by TSA or air traffic control.

No flights over nuclear facilities — In February 2003, an existing notice to airmen (notam) advising pilots not to circle or loiter over nuclear facilities was strengthened to reinforce the need for pilots to avoid these facilities altogether.

September 5, 2003

Aircraft Owners and Pilots Association
421 Aviation Way
Frederick, MD 21701
301-695-2162
www.aopa.org

[Top](#) [Printer Friendly Version](#)

Public section: [Home](#) | [Table of contents](#) | [About AOPA](#) | [Join or renew](#) | [What's new](#) | [Advocacy](#) | [AOPA Pilot magazine](#) | [Certified products](#) | [Air Safety Foundation](#) | [President's page](#) | [Learn to fly](#) | [Web links](#) | [Classified ads](#) | [Search](#)

Members section: [Register for access](#) | [Members home](#) | [Weather](#) | [Flight planning](#) | [Airport directory](#) | [Aircraft valuation service](#) | [Medical Information resources](#) | [Messaging/chat](#) | [Member profile](#)

Special access: [Airport Support Network](#) | [Press Center](#)

©1995-2003 Aircraft Owners and Pilots Association
[Our privacy policy](#) | [Contact AOPA](#) | [Terms of use](#)



WARNING:

**PILOTS REPORT ALL
SUSPICIOUS ACTIVITIES.**

1-866-GA-SECURE

National Response Center