Transportation Security Administration

Security Guidelines for
General Aviation Airport Operators and Users

June 2021

[Back of cover]

Table of Contents

EXECUTIVE SUMMARY **5**

1. BACKGROUND **6**

2. ABOUT GENERAL AVIATION **7**

3. GA VULNERABILITY **8**

4. INTRODUCTION TO RISK-BASED SECURITY **9**

5. GATHERING INTELLIGENCE **9**

5.1. IDENTIFYING THE THREAT 10
5.2. EIGHT SIGNS OF TERRORISM 10
5.3. PEOPLE 12
5.4. AIRCRAFT 12
5.5. INFRASTRUCTURE 12
5.5.1. Airport Security Assessment and Protective Measures Matrix 12

6. SUGGESTED AIRPORT SECURITY ENHANCEMENTS **13**

6.1. PEOPLE 14
6.1.1. Passengers/Visitors 14
6.1.2. Flight Schools/Student Pilots 14
6.1.3. Aircraft Renters 15
6.1.4. Transient Pilots 15
6.2. AIRCRAFT 15
6.3. INFRASTRUCTURE 16
6.3.1. Hangars 16
6.3.2. Locks 16
6.3.3. Key Control 18
6.3.4. Perimeter Security 18
6.3.5. Closed Circuit Television (CCTV) 19
6.3.6. Intrusion Detection Systems (IDS) 19
6.3.7. Fencing 19
6.3.8. Access points 21
6.3.9. Gates 21
6.3.10. Lighting 22
6.3.11. Signage 24
6.3.12. Identification System 24
6.3.13. Airport Planning 25
6.4. OTHER FACILITIES 25
6.4.1. Airport Tenant Facilities 25
6.4.2. Aircraft and Vehicle Fueling Facilities 26
6.4.3. Fuel Storage Equipment and Facilities 26
6.4.4. Military Facilities 27
6.4.5. Fixed-Base and Corporate-Based Operators (FBOs and CBOs) 27

7. AIRPORT WATCH PROGRAMS **28**

8. SECURITY AWARENESS TRAINING **30**

9. REPORTING PROCEDURES **30**

10. SECURITY PROCEDURES AND COMMUNICATIONS **31**

10.1. LOCAL AIRPORT SECURITY COMMITTEE 32
10.2. LAW ENFORCEMENT OFFICER (LEO) SUPPORT 33
10.3. NATIONAL TERRORISM ADVISORY SYSTEM (NTAS) 33
10.4. THREAT COMMUNICATION SYSTEM 33

11. SPECIALTY OPERATIONS **35**

APPENDIX A – AIRPORT SECURITY ASSESSMENT AND PROTECTIVE MEASURES MATRIX .. 36

APPENDIX B – AIRPORT SECURITY PROGRAM TEMPLATE 49

APPENDIX C – BOMB THREAT CALL CHECKLIST 53

APPENDIX D – BIBLIOGRAPHY 54

APPENDIX E – USEFUL WEBSITES AND CONTACTS 58

AVIATION TRADE ASSOCIATIONS 58

FEDERAL GOVERNMENT 58

FAA REGIONAL OPERATIONS CENTERS 58

OTHER REFERENCES 59

EXECUTIVE SUMMARY

This guidance document was developed jointly by the General Aviation (GA) community and the Transportation Security Administration (TSA). It is intended to provide GA airport owners, operators, sponsors, and entities charged with oversight of GA landing facilities, including tenants and/or users, with recommendations that address general aviation security concepts, technology, and enhancements. It provides a set of security best practices and a method for determining when and where these enhancements would be appropriate.

The application of recommended security enhancements is based on the general aviation community's analysis of perceived threats, areas of vulnerability, and risk assessments. This document does not contain regulatory language nor is it intended to suggest that any recommendations or guidelines should be considered mandatory. These recommendations and guidelines are not intended to suggest any specific or general criteria to be met in order to qualify for Federal funding. Program requirements for operators regulated under TSA's aircraft operator security rules (for example, Twelve-Five and Private Charter operations) are not addressed in this document.

These guidelines offer an extensive list of options, ideas, and suggestions for airport owners, operators, sponsors, and other entities charged with oversight of GA airports, including tenants and/or users to choose from when considering security enhancements for GA facilities. This guidance can enhance consistency across the nation with regard to security at GA facilities.

These guidelines also provide a method to determine security needs at different airports. Using a risk-based security approach, an airport operator can assess an airport's security characteristics and identify risks, threats, and vulnerabilities to decide which security enhancements would be most appropriate. The intent of this document is to provide a tool to enable GA airport managers to assess vulnerabilities and tailor appropriate security measures to their environment. Most threats can be categorized as follows: **Surveillance, Elicitation, Tests of Security, Funding, Supplies, Impersonation, Rehearsal, and Deployment**.

Members of the general aviation community identified eight functional areas of general aviation security. The functional areas include:

- Risk-based methodology
- Personnel
- Aircraft
- Infrastructure: Airports/Facilities [including fixed and corporate based operators (FBOs/CBOs)]
- Surveillance
- Security Plans and Communications
- Specialty Operations
- Tenants and Users

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

1. BACKGROUND

Following the 1988 Pan American World Airways Flight 103 tragedy, 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 TSA, to improve transportation security. Consistent with this mission, Congress transferred FAA's civil aviation security responsibilities to TSA. Accordingly, sponsorship of the ASAC was also transferred to TSA. The ASAC was permanently established pursuant to the Aviation Security Stakeholder Participation Act of 2014 (Pub. L. 113-238, Dec. 18, 2014; 49 U.S.C. § 44946), including a General Aviation subcommittee.

TSA requested the ASAC to develop guidelines for security enhancements at the nation's private and public use GA landing facilities. TSA believed that such an approach would be able to address GA airports (both public and private use) in a collaborative forum in order to develop a set of community-endorsed guidelines and "best practices" that are tailored to broad categories of airports and users.

The working group represented the GA community as a whole. Participating members included:

- Aircraft Owners & Pilots Association (AOPA)
- Airports Council International – North America (ACI-NA)
- 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)
- National Association of Flight Instructors (NAFI)
- National Agricultural Aviation Association (NAAA)
- United States Parachute Association (USPA)
- GA airport managers and representatives of various state government aviation agencies.

These security guidelines were initially developed as a collaborative effort between ASAC, GA stakeholders, and TSA to provide airport owners, operators, sponsors, and other entities charged with oversight of GA airports (including tenants and/or users), a set of mutually-endorsed security enhancements. This is a living document, initially released in May 2004, refined with input from stakeholders as needed. This version (Version 2) was developed with consideration of lessons learned and experience gained since 2004.

For the purposes of this document, "general aviation" and "airport" are defined as follows:

> **General Aviation (GA),** *as used in this document, encompasses all civil aviation, except military aviation, and scheduled or chartered passenger and cargo service under TSA security requirements in 49 CFR parts 1544 or 1546.*
>
> **Airport**, *as used in this document, means an area of land or water, or facility (heliport,*

hospital, drilling rig etc.) that is used or intended to be used for the landing and takeoff of aircraft, and includes its buildings and facilities if any. This document does not apply to airports required to comply with 49 CFR part 1542 or military airports.[1]

To date there have been numerous initiatives undertaken by the GA community, such as awareness programs, challenge and reporting methods, and educational courses. This document incorporates these programs by reference as appropriate to the topic. In addition, these guidelines recognize that every GA landing facility is unique. Therefore, the recommendations and guidelines contained in this document may be highly beneficial in one airport environment while being virtually impossible to implement at another. 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 operational environment.

This document does not contain classified or security sensitive information in order to enable its broad distribution to provide the greatest flexibility in creating an individualized template for all sizes of airports.

2. ABOUT GENERAL AVIATION

General aviation operations encompass a variety of activities, which include:

- Corporate/business aviation
- Personal/recreational flying
- Instruction/flight training
- Aerial application/crop dusting
- Aerial observation/search, rescue, law enforcement surveillance
- Air tours/air taxis
- Air medical/emergency services
- Skydiving/parachute operations

To accommodate this broad range of activities, and the equally broad range of related aircraft, GA airports vary in size, function, and operational characteristics. TSA understands that "one size of security" does not fit all GA airports. For example, a privately owned landing strip in a rural area may not need to implement the same security measures as a large, corporate airport near a major metropolitan area. While the potential for misuse of an aircraft operating from the rural airport exists, adherence to a single security requirement across the nation would be physically and economically unfeasible. Instead, these guidelines focus on providing measures to manage the risks associated with GA facilities in general, while recognizing the need to adapt these measures to the characteristics of each facility.

[1] Many airport terms used in this document 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. Using terminology that airport operators are already familiar with facilitates readers' understanding. Additionally, references to Federal Aviation Administration (FAA) guidance materials, while normally related to commercial service airports and operations, may not constitute an appropriate approach to security at GA airports.

Available general aviation statistics[2]:

- There are 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 operations of some commercial service airports.
- There are approximately 200,000 active GA aircraft in the U.S. that are responsible for 77% of all U.S. air traffic.
- GA aircraft range from one-person ultra-lights and powered parachutes with extremely limited range and payload capabilities to helicopters, seaplanes, vintage aircraft, fabric-and-wood biplanes, experimental airplanes, four-seat single-engine airplanes, twin turboprops, and large and small business jets.
- The GA community accounts for over 1.1 million jobs, with an economic impact that exceeds $219 billion annually.[3]
- There are approximately 600,000 certificated pilots in the U.S. Airmen Registry, most of whom conduct GA flight operations.
- Approximately 145 million passengers are transported annually in GA aircraft of all sizes, for business and personal reasons.
- An estimated 58% of all GA flights are conducted for business and corporate travel.
- Many commercial, non-scheduled flights (charters) are also a component of GA, with more than 22,000 pilots flying some 14,700 aircraft.
- Over 90,000 certificated flight instructors across the United States.

3. GA VULNERABILITY

Historically, civil aviation security regulations have not applied to GA airport operators and users. Before September 11, 2001, the Federal Government's role in airport security focused largely on those airports serving scheduled and public charter operations that required passenger screening. To date, TSA has not required GA airports to implement security measures except as necessary to provide enhanced security for the Washington, D.C. metropolitan area, including facilities located within the Washington, D.C. Metropolitan Special Flight Rules Area and gateway airports that are the last point of departure to Ronald Reagan Washington National Airport (DCA). Nevertheless, many GA airport managers and users commonly implement security measures similar to those found throughout the nation's commercial service airports. Examples include fencing, lighting, 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. Many general aviation aircraft operators also use secure lock and key controls to protect aircraft and hangar facilities similar to those used for commercial aviation.

These voluntary actions recognize that hardening one target (such as commercial aviation), may cause bad actors to look for softer targets. In other words, as vulnerabilities within other areas of aviation have been reduced, GA may be perceived as more susceptible to unauthorized use and, consequently, more vulnerable. The security guidelines outlined in this document are intended both as a resource to help GA airport managers and GA aircraft operators determine which

[2] US Federal Aviation Administration (June 2012). *Administrator's Fact Book*. Retrieved from http://www.faa.gov/about/office_org/headquarters_offices/aba/admin_factbook/media/201206.pdf

[3] Contribution of General Aviation to the US Economy in 2013 http://www.gama.aero/files/General%20Aviation%27s%20Contribution%20to%20the%20US%20Economy_Final_20150130.pdf

security measures they should employ to reduce vulnerabilities and as encouragement to adopt appropriate security measures that will provide a baseline of security for GA across the nation. The ability (physically and financially) of GA airports to voluntarily implement security improvements varies greatly. The majority of these facilities do not have finances and other resources at the level available to commercial service airports. Consequently, the considerations may not be the same, reflecting different concerns regarding economic feasibility, sustainability, and risk-reduction.

4. INTRODUCTION TO RISK-BASED SECURITY

The Department of Homeland Security (DHS) defines risk as "the potential for an adverse outcome assessed as a function of hazards/threats, vulnerabilities, and consequences;" using a consistent set of definitions for these terms:

> **Threat:** A natural or human-created occurrence which includes capabilities, intentions, and attack methods of adversaries used to exploit circumstances or occurrences with the intent to cause harm
>
> **Vulnerability:** A physical feature or operational attribute that renders an entity open to exploitation or susceptible to a given hazard
>
> **Consequence:** The effect of an event, incident, or occurrence [4]

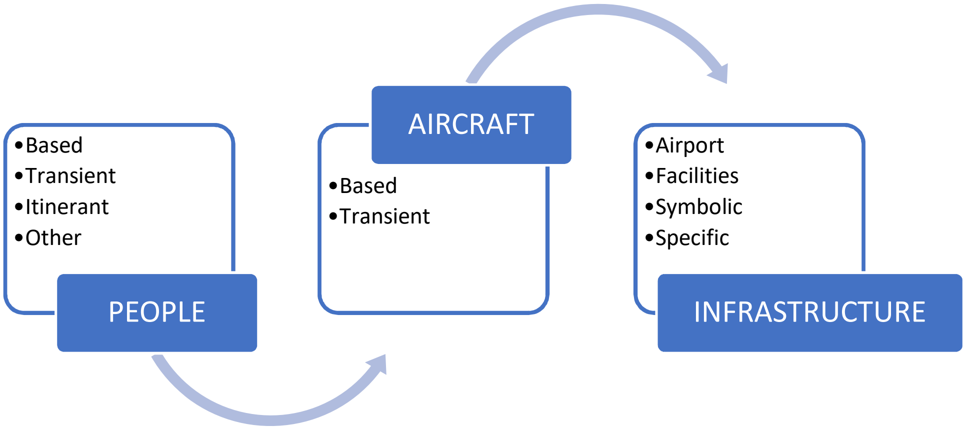
Within this context, risk-based security" (RBS) is a process that applies security measures, as appropriate for the risk to transportation security, based on an assessment of threats, vulnerabilities, and consequences. The RBS approach ensures that resources and requirements are focused on the areas were security enhancements are necessary to mitigate the risk.

5. GATHERING INTELLIGENCE

Developing a risk-based security program requires taking intelligence-based information and connecting the bits of data to one another to form a more complete picture to inform concepts and plans. TSA develops its programs and policies using information from the Intelligence Community (IC) regarding the threat as well as its knowledge of the industry to understand the vulnerability and potential consequences. GA operators rely on information provided by TSA, combined with other Federal, state, or local resources, and their own knowledge of their customers and the industry to make risk-based decisions. For example, a GA operator's long-term lease agreement and relationship with a hangar tenant of 30 years, or knowing a regular charter client with legitimate business interests around the region, provides a comprehensive picture that can constitute intelligence relevant to determining appropriate security measures. However, an operator with a new tenant, such as one who has only leased a hangar for two months, or a client who charters a jet for the first time, has limited data to derive an informed analysis. The difference in determining the level of risk between the two groups of clients is based on how much information or intelligence one has or needs to have in order to make a proper assessment.

[4] Source: *DHS Lexicon, Terms and Definitions* (2016 Edition)

The strength of any security mechanism is dependent on the airport's overall security plan. For example, perimeter control methods alone do not necessarily prevent access to a determined intruder, nor are they appropriate for every facility. Airport operators should consider facility-specific security measures and make decisions based on the cost-effectiveness for the airport's overall security posture. For example, at certain airports perimeter security fencing may be cost prohibitive and other options for securing aircraft, such as chock locks, may be more effective from a cost/benefit standpoint.



5.1.Identifying the Threat

Before GA operators can understand their vulnerabilities, they must understand the threat. While many potential targets and scenarios exist, most security experts, GA operators, and the IC agree that the use of an aircraft for an attack on a specific target is the dominant threat related to general aviation[5]. Other concerns range from acts perpetrated by lone operators to large business aircraft of foreign origin carrying unknown contraband, including nuclear materials or weapons. General aviation aircraft may be stolen, hijacked, and/or modified to serve as Vehicle Borne Improvised Explosive Devices (VBIEDs). In some cases, the aircraft could be targets, whether in flight or on the ground. Finally, light or small aircraft should not be dismissed as a threat merely because their casualty potential is low—the infliction of terror alone, or the resulting economic impact, could be sufficient to achieve a terrorist's goals. However, in each instance, the interface is always human; the thief, the hijacker, the bomb-maker, or the terrorist who just wants to know how to fly the airplane but not necessarily know how to land it[6].

5.2.Eight Signs of Terrorism

In their engagement with customers and passengers, GA operators have the opportunity to assess and identify potential threats. In general, it is a matter of knowing your industry and knowing your customers, then using that knowledge to identify anomalies or aberrant behavior. There are several activities that are possible indications of terrorist activity.

[5] The IC is equally concerned with the take-down of a civilian aircraft having inadvertently entered into a flight restricted area without being able to accurately determine if the aircraft actually posed a threat.

[6] While TSA has not seen sufficient intelligence information regarding threats to warrant mandatory measures, owners and operators should be alert to the potential for terrorist activity.

1. **Surveillance—**Person(s) discretely recording or observing operational activity. This may include the use of video recorders, cameras, note taking, drawing diagrams, marking maps, using vision-enhancing devices such as telescopes or binoculars, or using small Unmanned Aircraft Systems (UAS).

2. **Elicitation—**Person(s) or organizations trying to gain information about law enforcement, security, or other capabilities, operations, or people. Types of elicitation may involve eavesdropping, friendly conversation, and asking (direct) questions, including asking about airport operations. Elicitation may also be conducted via mail, email, and viewing websites. Other examples could include unusual or prolonged interest in or attempts to gain sensitive information about security measures relating to personnel, entry points, peak activity, hours of operations, heating/ventilation/air-conditioning (HVAC) systems, and access control aids such as alarms and locks.

3. **Tests of Security—**Attempts to measure reaction times to security breaches, including decay in response times; attempts to penetrate physical barriers, including airport perimeter fencing, rooftops, and other sensitive areas; or attempts to assess strengths and weaknesses by monitoring procedures. This may include fictitious emergency calls to the same locations or venues.

4. **Funding—**Suspicious transactions involving large ***cash*** transactions, such as when purchasing fuel or even aircraft.

5. **Supplies—**Purchasing or stealing, and storing large quantities of explosives or explosive-making materials, weapons, munitions, chemicals or biological agents etc., that may seem out of place or context. This activity is usually associated with person(s) going out of their way to avoid contact; conducting suspicious activities, keeping doors closed and windows blacked-out, as well as making unusual modifications to aircraft to disperse or release Improvised Explosive Devices (IEDs) or agents.

6. **Suspicious people—**Person(s) who seem out of place. This may include impersonating pilots, airport line personnel, law enforcement, security, or employees of companies, including using fake badges or vehicle decals.

7. **Rehearsal—**Positioning and moving people around without actually committing a terrorist act. This may include activities such as mapping out routes, driving on uncontrolled aircraft ramps, or timing distances and traffic signals.

8. **Deployment—**Person(s) moving into position to commit a terrorist act. This is the last chance to thwart an act of terrorism.

In applying RBS to the GA community, the focus is, first and foremost, on ***people*** we do not know[7]. Secondly, the focus is on ***aircraft*** that are not secure. And finally the focus is on protecting ***infrastructure***, including the airport, an FBO, flight school, or other GA service provider.

[7] The balance between privacy and security is an all-important concern; an individual's privacy and constitutional rights should never be violated.

5.3.People

The first step of RBS for GA is to determine if there is sufficient information to make a risk assessment. If there is not, then determine what additional information is needed to make a decision that could allow a subject to be cleared for access or employment. This includes basic information on customers with operating agreements and permits, as well as employees; itinerant clients such as student pilots, limo drivers; and others who provide ancillary support such as fuel truck drivers, and package delivery companies.

Potentially suspicious activities include transient customers who give off indicators that "something may be wrong", such as pilots who paid cash for fuel or an aircraft tail-number that appears altered. Any one indicator is not necessarily a concern, but in combination may warrant additional scrutiny. A risk assessment may be cursory or more involved, depending on the situation, with a focus on people and things about whom or which little is known.

It is not necessary to have complete information on all users as long as there is credible reliance on responsibility by all GA security partners. Operators at an airport include airport operators, aircraft operators, FBO, and other facilities at an airport. While an airport may not need to know the client list of an FBO, it needs to be confident that the FBO has the necessary information. The same applies to the GA aircraft operator's employees and the knowledge that each employer has vetted them.

5.4.Aircraft

The next stage is to take reasonable steps to secure aircraft. This process is more prescriptive in nature. It may involve locking, immobilizing, or preventing movement of an aircraft and ensuring proper control and custody of keys, as further described in this document.

5.5.Infrastructure

The final stage is securing the airport and facilities as potential targets. All GA airports, landing facilities, and operators, regardless of size, are assumed to bear some level of risk and the airport operator is responsible for assessing that risk and mitigating the same. A checklist of airport facilities and airport infrastructure called the "Protective Measures Matrix" is included in Appendix A and can be useful tool in assessing risk.

5.5.1. Airport Security Assessment and Protective Measures Matrix

The intent of the airport security assessment is to establish a baseline report from which to develop security measures to prevent the unauthorized use of aircraft; to protect the health and welfare of tenants, users, and employees at the airport; and, as a critical asset to the region, to protect the airport from being degraded.

Since September 11, 2001, there is a greater awareness that terrorists wish to do harm to the way of life in the U.S., and it has become necessary to increase vigilance to protect people and assets. Aviation continues to be of significant interest to terrorists and all aspects should be considered potential targets, including but not limited to the use of aircraft as weapons of mass destruction; aircraft as means of conveyance of people, cargo, weapons, or materials; airport facilities and other airport assets; and, last but not least, passengers, tenants, users and employees at airports. The Protective Measures Matrix template (included in Attachment A) is designed primarily for assessment of general aviation but may have broader applications, with modifications, to commercial aviation and other critical sectors.

Airport security is risk-based if it is *layered, intelligence-driven,* and *prescriptive*, that is it responds to a known or potential threat or addresses a security vulnerability. For example, risk-based security has long been applied in the GA sector by asking "is the behavior consistent with the expected norm?".

Security measures should consider the three elements of risk: threat, vulnerability, and consequence. In open societies, especially where the public is invited to engage in a wide range of activities including commercial activity, some level of risk is always present when balancing security needs against convenience and the freedom to operate. While no program can be 100 percent secure and each airport and situation is unique, requiring its own assessment and mitigation processes, it is up to policy makers and airport management to decide how limited resources are allocated to secure the airport while continuing to operate as a public facility.

The matrix example included in Appendix A of this document identifies (a) pre-event preparedness, (b) detection and response during an event, and (c) post-event recovery, using a subjective 0-5 point scoring system.

6. SUGGESTED AIRPORT SECURITY ENHANCEMENTS

These guidelines contain security enhancements that may be appropriate for those facilities scoring low on the Airport Security Assessment and Protective Measures Matrix. The guidelines 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 many locations, but 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.

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

- Personnel
- Aircraft
- Infrastructure: airports/facilities (including fixed and corporate based operators (FBOs/CBOs)
- Surveillance
- Security Plans and Communications
- Specialty Operations
- Tenants and Users

6.1.People

6.1.1. 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 meet with the pilot or other flight department personnel in advance of any flights. Suspicious activities -- such as use of odd payments 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 to escort individuals visiting the airport into and out of aircraft movement and parking areas, when appropriate. Prior to boarding, the pilot in command should ensure that:

- The identity of all passengers is verified;
- All passengers are aboard at the invitation of the aircraft owner/operator; and
- All baggage and cargo is identified by the passengers or flightcrew.

Aircraft operators may also consider, as a recommended practice, the development and use of an internal "vetted traveler" type program, which includes the successful and favorable completion of a background check before being added to a list of individuals approved for travel aboard company aircraft.

6.1.2. Flight Schools/Student Pilots

We know that several of the September 11th terrorists trained at flight schools in Florida, Arizona, and Minnesota. This raised concerns among the public and Federal law enforcement organizations about flight school security and how it can be improved. All aliens (as defined in the Immigration and Nationality Act) taking flight training with a U.S. certificated flight instructor or at a U.S. certificated flight school are subject to a background check in accordance with the requirements established in 49 U.S.C. § 44939 and 49 CFR 1552. Each U.S. certificated flight instructor and U.S. certificated flight school must ensure its employees have completed security awareness training, as required in 49 CFR part 1552 subpart B. Additional information about flight training requirements is available online at https://www.flightschoolcandidates.gov.

In addition to the Federal statute and regulations, the following procedures are recommended to ensure positive control of the training aircraft before movement:

- 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.
- Consider having any student pilot check in with a specific employee (for example, dispatcher, aircraft scheduler, flight instructor, or other management official) before

being allowed access to parked aircraft.

- 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.
- Have the student sign or initial a form and not receive keys until an instructor or other management official also signs or initials.
- Use a different ignition key from the door lock key when practicable. The instructor would provide the ignition key when he or she arrives at the aircraft.

6.1.3. Aircraft Renters

At most airports, regular aircraft renters are fairly well known, and new renters are typically required to complete a flight check, which ascertains their ability and appropriate certification level to safely operate rental aircraft. While both of these factors may serve as a deterrent to GA aircraft being used for nefarious purposes, developing and documenting standard procedures and ensuring flight school employees are educated in those 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 their security responsibilities at the facility.
- Operators providing rental aircraft should be vigilant for suspicious activities and report them to appropriate officials.
- Operators providing rental aircraft can assist in security awareness and provide awareness training to renters. See also Security Awareness Training.

6.1.4. Transient Pilots

Airport personnel should strive to establish procedures to identify any pilots and aircraft using their facilities who are not normally based there. 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. Assigned parking spots or transient parking areas can help to easily identify transient aircraft on an apron.

6.2.Aircraft

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

Methods of securing aircraft include:

- Ensuring that door locks are consistently used to prevent unauthorized access or tampering with the aircraft
- Using keyed ignitions where appropriate
- Controlling access to the keys
- Storing the aircraft in a hangar, if available, and locking hangar doors
- Using an auxiliary lock to further protect aircraft from unauthorized use
- Using commercially available options, such as locks for propellers, throttle, and tie-downs
- Ensuring that aircraft ignition keys are not stored inside the aircraft
- Discussing transfer of control for before and after maintenance procedures to avoid leaving aircraft open with keys in between the "hand-off"
- Using heat shields and aircraft covers to block the window to prevent easy visibility of the aircraft's contents

6.3.Infrastructure

6.3.1. 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 in accordance with local codes. 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 enhanced security measure, in addition to locking hangar doors, an electric bypass switch and/or alarm and intrusion detection systems could also aid in the security of hangars.

Commonly, tenant lease agreements allow airport management to have access to all hangars to inspect hangars, and other leased space in the event that inappropriate activities are suspected.

When building new hangars, consider the materials used and how entry doors are framed. The material should not be so weak that the door could be easily pried open.

6.3.2. Locks

Locks are an integral part of security. In addition to their functional deterrence, their physical strength and resistance to all but the most determined thief provides security in itself. However, many ingenious methods have been developed to open locks surreptitiously. Some locks require considerable time and expert manipulation for covert opening, but all 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. The additional time required to overcome the lock and usual added noise provides an increase in the probability of detection.

An important consideration when investing in airport equipment, such as locks, is total life cycle costs, not merely the initial capital cost. 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, these locks may not be suitable for outdoor use if they will be exposed to freezing temperatures and precipitation. 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 because lock codes can be given to unauthorized users and the presence of other personnel could deter the unauthorized use of the code. 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 when a tenant moves out.

- Advanced electronic key technologies - These systems provide a number of benefits to airport security. 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 user's movements throughout the airport area.

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 need to use the lock (for instance, would a combination be better than issuing keys)?

- Would a certain type of lock unnecessarily impede access in high traffic areas?

- How secure should the area be made?

- Is the area monitored?

- How often do codes, keys, or locks need to be changed for persons needing access (for example, new hangar tenants, those with tie down agreements needing ramp access, etc.)?

- Will use of a lock interfere with fire code egress requirements?

Deadbolt locks, built-in door handle locks, or padlocks and metallic keys should be considered to secure an access point, particularly those that are perceived or presumed to be low-risk, low throughput, or significantly distant from the main areas of concern. Such locking systems may involve other procedural issues, such as a key management system. Look for key management systems that easily record numerous access points and maintain accurate records of reissuing keys when they are lost or stolen.

6.3.3. Key Control

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. Lock and key control guidelines should include:

KEY CONTROL
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.

- Where 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 need 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 (recommended at least annually) audited to ensure accountability for all keys.

6.3.4. Perimeter Security

To delineate and adequately protect security areas from unauthorized access, it is important to consider boundary measures such as fencing, walls, electronic boundaries (for example, sensor lines, alarms), and other physical 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 safety and 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. Natural barriers, such as ditches or other natural breaks, can be operationally and financially effective.

6.3.5. Closed Circuit Television (CCTV)

Although CCTV is used for many purposes, its most common use is for surveillance or as a visual record. Monitored CCTV systems make it possible for fewer individuals to maintain a constant watch on all areas of the facility. If appropriately monitored, these systems may be an effective method of perimeter security. In conjunction with a perimeter fence, CCTV may deter security breaches at airports and may provide an improved response when breaches do occur. But they must be staffed at the level necessary for consistent and careful monitoring to identify suspicious activity while it is occurring.

Additionally, CCTV video recorders may provide a visual record that can be used to document activities that become the subject of investigations. CCTV, as well as "smart-CCTV" (video analytics) may be appropriate only at busier, more complex airports.

Airport operators and tenants, should consider outdoor security lighting and cameras to help improve the security of:

- Aircraft parking and hangar areas
- Fuel storage areas and fuel trucks
- Airport access control points
- Other appropriate areas, such as vehicle parking, fences, or obstructed areas

6.3.6. Intrusion Detection Systems (IDS)

Intrusion detection systems are becoming increasingly popular for GA airport security use. 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, a contracted company constantly monitors such systems. If an intrusion or some other specified event (for example, 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 at terminals, hangars, or other airport facilities, or be used to monitor perimeter security and access points.

6.3.7. Fencing

Security fencing is the most common means of securing a perimeter. Fencing design, height, and type can vary depending on local security needs. Typically, fences are low-maintenance, provide clear visibility for security patrols, provide added safety by deterring animals from sensitive areas of the airport, 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 many 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 based 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 may not discourage a determined intruder; it can serve to alert airport management to the presence of unauthorized individuals. To derive the most value, a fencing system should be used in conjunction with a “challenge” system or airport watch program.

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 some airports. Partial fencing of sensitive areas such as aircraft storage or maintenance areas may be more appropriate and can prove to be just as effective.

The physical barrier provided by a fence creates the following security advantages:[8]

- Gives notice of the 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
- 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

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 - prevents individuals from crawling under the fence line
- 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

[8] Source: Chain Link Fence Manufacturer’s Institute.

- 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, utility poles; nor areas with stackable crates, pallets, storage containers, or other materials abutting the fence line. Likewise, the parking of vehicles along the fence line 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.

Airport operators should be careful that increased perimeter controls and measures do not prevent authorized personnel from gaining airfield access such as fire and emergency response vehicles.

Additional information on materials and installation is available from the following sources (also see Appendix D – Bibliography):

- FAA Advisory Circular Part 1500 Series AC 150/5360-13, Planning and Design Guidelines for Airport Terminal Facilities

- AC 150/5370-10, Standards for Specifying Construction of Airports, DOT/FAA/AR-00/52

- TSA's Recommended Security Guidelines for Airport Planning, Design, and Construction

- The Chain Link Fence Manufactures Institute and American Society for Testing and Materials (ASTM).

6.3.8. 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. 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 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.

6.3.9. Gates

Gates are the only moveable part of a fence and therefore should be properly constructed with appropriate fittings. Chain link gate specifications are included in industry and federal guidance documents listed in Appendix D - 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 inches of ground clearance beneath the gate and minimal gaps on both sides of the gate.

6.3.9.1. Vehicle Gates

At vehicle access gates, the chief concern is tailgating, especially 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 gate and signage should be designed to allow practical and efficient use of the gate by authorized users and to prevent tailgating in a safe and non-confrontational manner. It is the responsibility of each authorized person to prevent tailgating; and where prevention is not practical or safe, to report suspected unauthorized access. Signage should remind vehicle operators to confirm gate closure.

In order to make prevention of tailgating practical and safe, gates and corridors should be designed to allow only one vehicle to pass at a time – even when the leading vehicle has pulled forward to allow the gate to close. Limiting the size of the opening increases security, reduces the possibility of one vehicle passing another, and shortens the open/close cycle time. The delay for gate closure should be minimized; unnecessarily long waits tempt even the most conscientious users.

The cantilever slide gate is very effective for vehicle security, especially if electrically operated. An automated two-gate system (also known as vehicle entrapment gate) is another 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 using security equipment that provides space for waiting vehicles to stop to obstruct or deter other vehicles from passing through.

6.3.9.2. Pedestrian Gates

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.

6.3.10. Lighting

Protective lighting provides 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 and pedestrian access

- Detection of unauthorized access/intruders
- Deterrence of illegal activity

Protective lighting is generally inexpensive to maintain and, when properly employed, may provide airport personnel with an increase in detection and decrease in response time to 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 lighting to help improve the security of aircraft parking and hangar areas, fuel storage areas, airport access points, and other appropriate areas.

Good protective lighting is achieved by using 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 includes 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 pedestrian or vehicle 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 employing this system:
    - Glare projection lighting where the glare of lights directed across surrounding territory do not annoy 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 (such as proximity, photoelectric, or timers) lighting may be considered in areas which have minimal traffic throughput in the off-peak hours.

6.3.11. Signage

NO TRESPASSING
STATE LAW PROHIBITS UNAUTHORIZED ENTRY, TAMPERING WITH AIRPORT FACILITIES, OR TAMPERING WITH AIRCRAFT.
VIOLATORS WILL BE FINED AND/OR IMPRISONED.

Signage provides a deterrent by warning individuals of facility boundaries and 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.

Wording may include, but is not limited to warnings against trespassing, unauthorized use of aircraft and tampering with aircraft, and reporting of suspicious activity. Use as concise language as possible. Signage should include phone numbers of the nearest responding law enforcement agency, 9-1-1, or TSA's 1-866-GA-SECUR, as appropriate.

Many locations with access control or Closed Circuit Television (CCTV) equipment may warrant signage for directional, legal, or law enforcement purposes, such as:

"NOTICE: All activities in this area are being monitored and recorded"
"ALARM WILL SOUND IF OPENED"
"AUTHORIZED PERSONNEL ONLY"

For more information, refer to FAA Advisory Circular (AC) No: 150/5360-12E, 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.

6.3.12. Identification System

Airport operators may consider implementing a method of identifying authorized individuals in various areas of the airport. Currently, there are many systems on the market to 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, accountability, and integrity 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's name

- A unique identification number
- The scope of the individual access and movement privileges (for example, color coding)
- A clear expiration date

In addition to FAA safety standards for vehicles entering movement and non-movement areas of the airport, an airport operator may consider a method of identifying authorized vehicles entering restricted areas. Such a system can assist airport personnel and law enforcement in identifying unauthorized vehicles. Vehicles can be identified through the use of decals, stickers, or hang tags. Decals should be nontransferable; that is, removing the decal should destroy its integrity and prevent re-use. 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 Title 49 CFR Parts 1542 and 1544.

6.3.13. 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. TSA, in coordination with aviation industry, developed Recommended Security Guidelines for Airport Planning, Design, and Construction in 2017. The purpose of the document is to provide an extensive list of options, alternatives, ideas, and suggestions for the airport architect, designer, planner, and engineer to choose from when considering security requirements in the early planning and design of new or renovated airport facilities.

The Federal Emergency Management Agency (FEMA), Department of Defense (DOD), and Department of State (DOS) have issued a number of publications on antiterrorism design standards for buildings, perimeter barriers, and vehicle gates. Reference Appendix D – Bibliography.

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 minimum standards documents or individual development guidelines. In addition, airport construction projects can affect airfield security. Construction personnel and vehicle access during projects should also be considered.

6.4. Other Facilities

6.4.1. Airport Tenant Facilities

For those airports with a perimeter fence, many airport tenant facilities have access to the aircraft parking, 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.

The National Business Aviation Association has developed a list of best security practices. These include:[9]

- Ensure facility perimeter security with effective fencing, lighting, security patrols (as appropriate), gates, and limited access areas
- Ensure street-side gates and doors are closed and locked at all times
- Require positive access control for all external gates and doors
- Close and lock hangar doors when that area is unattended
- Secure key storage areas (food and liquor, parts and tools, etc.)
- Use an access control management system for keys and passes
- Confirm the identity and rightful presence of each passenger, vendor, and visitor prior to allowing access to facilities and aircraft
- Use a government issued photo ID to verify identity of any visitor or vendor
- Escort all visitors on the ramp and in the hangar area
- Post emergency numbers prominently around facility
- Ensure easy access to phones or "panic buttons" in various facility locations (break room, hangar bay, etc.)
- Confirm security of destination facilities
- Be aware of your surroundings and do not be complacent—challenge strangers

6.4.2. Aircraft and Vehicle Fueling Facilities

Fuel farms are normally placed in as remote a location of the airport as possible. If feasible, security fencing, lighting, and access controls should be used 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 marshaling fuel trucks in an easily monitored location.

6.4.3. Fuel Storage Equipment and Facilities

- Keys to fuel trucks should be removed from the vehicle when parked in unmonitored areas, during times when the parking area is unmonitored (for example overnight), or when required by the airport.

[9] NBAA (2013). Best Practices for Business Aviation Security (NBAA). Retrieved from https://www.nbaa.org/ops/security/best-practices/

- Fuel storage facilities should be fenced and/or monitored to prevent unauthorized access.

- Valves or controls of fuel storage tanks, piping, or pumping mechanisms should be locked when not being used, unless access is restricted per the recommendation above.

- Inspection schedules should be created for fuel storage facilities.

6.4.4. 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 often these facilities may be at least partly within the military 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.

6.4.5. Fixed-Base and Corporate-Based Operators (FBOs and CBOs)

In addition to complying with applicable airport security procedures and evaluating the recommendations contained in this document, FBOs and CBOs should consider establishing the following guidelines for ramp access by non-airport personnel and third-party vehicles, and fuel storage equipment.

Ramp Access by Non-Airport Personnel Flight Crew for Non-Based Aircraft: An FBO/CBO employee should verify the identity of the aircraft crew before allowing access to the ramp, hangar, or aircraft.

Passengers: Enplaning passengers should be positively identified by the aircraft crew before they gain access to the ramp. Deplaning passengers should be directed and escorted safely to the terminal by a crewmember or FBO/CBO employee, taking care to avoid aircraft that are in the process of starting engines, parked with engines running, or beginning to taxi off the ramp.

Others: Vendors, contractors, and visitors should be positively identified by an FBO employee before being allowed access to the ramp. The FBO/CBO should develop guidelines that determine when the vendor, contractor, or visitor needs to stay under direct surveillance by an FBO/CBO employee or authorized representative.

Ramp Access by Third-Party Vehicles: The FBO/CBOs should develop an access policy for third-party vehicles (for example, vehicles not driven by employee of any operator, user, or tenant). The policy should provide control mechanisms appropriate to the airport characteristics and potential risks. Examples of control mechanisms are listed below, although it may not be necessary for all of them to be enacted in order for the policy to be effective. Note that some of these control mechanisms may not be feasible at airports without fencing and access gates.

- Verifying the identification of the driver and/or passengers prior to allowing access

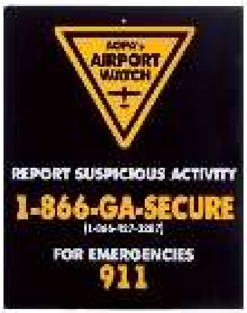
- Recording the identification of the driver and /or passengers on a ramp access log

- Verifying destination and need for access:
  - Flight crew verification of passengers (for example, a sedan taking passengers to awaiting aircraft)
  - Work order (in example of contractor/construction vehicle)
  - Bill of lading (in example of delivery of supplies or equipment)
- Monitoring the vehicle – either an “escorting” company vehicle, on foot, or via CCTV – during part or all of the time the third party vehicle in on the ramp.
- Restricting access to certain types of vehicles (for example, ambulances, sedans/car service, utility or contract trucks, etc.)

The FBO/CBO should always prohibit access to any vehicle without a legitimate need to be on the airport ramp area.

7. AIRPORT WATCH PROGRAMS

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 noticed quickly. 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. Pre-existing programs that can be used include the Aircraft Owners and Pilots Association’s (AOPA) Airport Watch[10], the DHS “If You See Something, Say Something”[11] campaign, or the TSA “This is My Airport” campaign.



Airport-Specific Watch Programs

The following should be considered for an airport watch program, along with additional measures specific to each airport:

- Coordinate the program with all appropriate stakeholders including airport officials, pilots, businesses and/or other airport users
- Hold periodic meetings with the airport community
- Educate the airport community on proper reporting procedures for suspicious or unusual persons or activities, per information contained in the following sections
- Develop and circulate challenge and reporting procedures to all who have a regular

[10] Aircraft Owners and Pilots Association (2013). *Airport Watch*.
[11] Available at https://www.dhs.gov/see-something-say-something

presence on the airport

- Encourage proactive participation in aircraft and facility security and heightened awareness measures
- Encourage airport and line staff to challenge and report unknown individuals 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 security awareness training to all involved for recognizing suspicious activity and appropriate response tactics

Human Trafficking

In recent years, there has been much attention given to general aviation in regard to human trafficking. Although commercial aviation has also been utilized to facilitate human trafficking, the potential for greater privacy and security screening avoidance can make general aviation a viable method to transport victims versus traditional commercial travel.

Human trafficking involves the use of force, fraud, or coercion to obtain some type of labor or commercial sex act. Every year, millions of men, women, and children are trafficked worldwide – including right here in the United States. It can happen in any community and victims can be any age, race, gender, or nationality. Traffickers might use violence, manipulation, or false promises of well-paying jobs or romantic relationships to lure victims into trafficking situations.

Language barriers, fear of their traffickers, and/or fear of law enforcement frequently keep victims from seeking help, making human trafficking a hidden crime.

Traffickers use force, fraud, or coercion to lure their victims and force them into labor or commercial sexual exploitation. They look for people who are susceptible for a variety of reasons, including psychological or emotional vulnerability, economic hardship, lack of a social safety net, natural disasters, or political instability. The trauma caused by the traffickers can be so great that many may not identify themselves as victims or ask for help, even in highly public settings.

Many myths and misconceptions exist. Recognizing key indicators of human trafficking is the first step in identifying victims and can help save a life. Not all indicators are present in every human trafficking situation, and the presence or absence of any of the indicators is not necessarily proof of human trafficking.

The safety of the public as well as the victim is paramount. Do not attempt to confront a suspected trafficker directly or alert a victim to any suspicions. It is up to law enforcement to investigate suspected cases of human trafficking. To report suspected human trafficking, contact the Homeland Security Investigations Tip Line at 1-866-347-2423.

The information above was taken from the DHS Blue Campaign website. The Blue Campaign is a national public awareness campaign designed to educate the public, law enforcement, and other industry partners to recognize the indicators of human trafficking, and how to appropriately respond to possible cases. More information, including indicators and ways to report suspicious behavior, can be found on the website: www.dhs.gov/blue-campaign

The DHS Blue Campaign partnered with the U.S. Department of Transportation to create the Blue Lightning Initiative (BLI). BLI trains aviation personnel to identify potential traffickers and human trafficking victims, and to report their suspicions to federal law enforcement. BLI partners with the commercial and general aviation industry to train staff on common indicators and the reporting protocol. To learn more about becoming a BLI partner, and to access the tools made available through the BLI email bluecampaign@hq.dhs.gov.

8. SECURITY AWARENESS TRAINING

TSA developed a security awareness training program for use by the general aviation community. The training program provides information on suspicious behavior patterns, appropriate responses to such behavior, and GA airport watch programs. The training program is available by contacting TSA Headquarters via email at TSAGeneralAviation@dhs.gov. The AOPA GA Security Online Course[12] provides similar security awareness training and is highly recommended. Airport users should always report any suspicious activity to their direct supervisor, airport, or law enforcement official.

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.

9. 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 two ways that persons can report

[12] Retrieved from http://flash.aopa.org/asf/gasecurity/gasecurity.cfm?

suspect activities.

1. In all cases involving critical and immediate incidents or threats, contact 9-1-1 local Emergency Dispatch.

2. For incidents or situations that are not immediate or critical, bring them to the attention of the airport operator who can often satisfy and resolve questions regarding the legitimacy of an activity.

3. A third method is to utilize the GA-SECURE hotline. TSA developed and implemented a GA hotline in partnership with the National Response Center. The toll-free number is (866) GA-SECUR (1-866-427-3287) 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. In addition, a Suspicious Activity Report (SAR) may be filed with a regional information analysis fusion center. Most states have information/intelligence analysis fusion centers staffed by Joint Terrorism Task Forces (JTTFs) focused on connecting the dots between incidents and disseminating the information to law enforcement around the country in the event of suspicious patterns, for example, the "8 Signs of Terrorism."

What to report:

- Suspicious activity or type of incident
- Date and time
- Aircraft registration, or "N" number, or airport location
- Physical appearance of suspicious person(s) (gender, height, clothing)
- Other relevant information

10. SECURITY PROCEDURES AND COMMUNICATIONS

General aviation airport managers/operators may find it helpful to develop written security procedures. Many of these security initiatives are already being conducted at airports 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 measures. 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 programs. Because security procedures may contain sensitive information, the airport operator should limit access to them to the extent possible and follow local, state, or Federal law as appropriate, or airport-established protocols to restrict access.

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 airport 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 the National Terrorism Advisory System (NTAS) 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, state, and federal agency representatives such as DHS, FBI, and TSA.
- Conduct asymmetric surveillance of facility property, buildings, and aircraft.
- Coordinate emergency plans as appropriate with nearby hotels, local hospitals, Red Cross, and other local jurisdictions and agencies.
- Hold security committee meetings to ensure timely dissemination of security/threat information.
- Encourage participation in simulated emergencies by tenants and employees to ensure preparedness.

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

- Continuing to conduct all measures taken at lower threat alert conditions
- Limiting facility access points
- Making random and unpredictable/asymmetric surveillance patrols of facility property, buildings, and aircraft by varying times, routes, vehicles, personnel, and any other associated activity.
- 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 mobilizing specially trained teams or resources
- Closing the facility

10.1. Local Airport Security Committee

Airport management should consider establishing a local airport security committee. This committee should be composed of airport businesses, 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.

10.2. Law Enforcement Officer (LEO) Support

Airport operators should 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. TSA's Visible Intermodal Prevention and Response (VIPR) teams, in particular, can be valuable partners for airport operators. VIPR teams are specifically authorized by statute to enhance security through law enforcement and screening capabilities in all modes of transportation, including airports.

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 (for example, airport ID badges, airmen certificates)
- Recognizing those airport users authorized to drive on the ramp
- Information about how the LEOs can obtain airport access (for example, who has gate keys, access codes)
- Airport speed limits, aircraft right-of-way procedures, and other "normal" operations
- Issuing airport maps with a detailed facility index recognizing "normal" airport operations.

10.3. National Terrorism Advisory System (NTAS)

The Department of Homeland Security's NTAS is a mechanism 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. Additional information can be found at www.dhs.gov/national-terrorism-advisory-system.

10.4. 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 to all appropriate individuals and their alternates. The following phone numbers should be included on the contact list (include after hour contact numbers where appropriate):

- Airport operator
- Airport 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
- Transportation Security Operations Center (TSOC)
- Federal Bureau of Investigation
- Local FAA contact[13]
- Local TSA contact (ex: Federal Security Director or designee)
- Tenants
- 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, for example 800 MHz radio systems.

Also important to the communication process is a means by which all current 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 GA community to discuss security issues and challenges, establishing a centralized area for posting of security information, or even developing an email alert system.

[13] Appropriate local FAA contacts include Air Traffic Control, FAA Regional Operation Center (ROC), and/or local Law Enforcement Assistance Program (LEAP) special agent. See Appendix E for ROC contact list

11. SPECIALTY OPERATIONS

Agricultural Aircraft Operations

While many agricultural aircraft operators have taken proactive steps to secure the general aviation community, in order to establish a consistent baseline of security, owners/operators should take appropriate steps to ensure their security measures secure agricultural aircraft when unattended, including:

- Using 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.
- Ensure that containment facilities for chemicals are secured with locks; ensure Material Safety Data Sheets are available for all chemicals.

Additional security measures [14]can be found on the National Agricultural Aviation Association website.

[14] Kansas State University (March 2002). *Agricultural Aviation Security*. Retrieved from http://www.agaviation.org/sites/default/files/Agricultural_Aviation_Security-EP111.pdf

APPENDIX A – AIRPORT SECURITY ASSESSMENT AND PROTECTIVE MEASURES MATRIX

This airport security assessment was conducted on behalf of [INSERT AIRPORT NAME] by _______________________________________ on MM/DD/YY.

INSTRUCTION: The intent of this airport security assessment is to establish a baseline from which to develop security measures with the intent of preventing the unauthorized use of aircraft; to protect the health and welfare of tenants, users and employees at the airport; and, as a critical asset to the region, to protect the airport from being degraded.

The following matrix identifies (a) pre-event preparedness, (b) detection and response during an event, and (c) post-event recovery, using a "subjective" scoring system from 0-5. The scoring is subjective due to the individual biases and assumptions the person(s) conducting the assessment may have, for example, "in the opinion of." No composite or weighted scores are applied because it is layered risk-based security and each link, regardless of strength, contributes to overall security.

Because this assessment, when completed, may contain Sensitive Security Information (SSI), the airport operator must control access in accordance with 49 Code of Federal Regulations (CFR), Parts 15 and 1520.

BACKGROUND: Since September 11, 2001, there is a greater awareness that terrorists abroad and in the Homeland wish to do harm to the way of life in the U.S., and it has become necessary to increase vigilance and protect the health and welfare of people, as well as protect critical assets from being operationally degraded. Aviation continues to be of significant interest to terrorists and all aspects should be considered potential targets, including but not limited to the use of aircraft as weapons of mass destruction—irrespective of size; aircraft as means of conveyance of people, cargo, weapons or materials; airport facilities and other airport assets; and, last but not least, passengers, tenants, users and employees at airports. The protective measures matrix template that follows is designed primarily for general aviation, but may have broader applications, with modifications, to commercial aviation and other critical sectors.

Airport security should be *layered, risk-based, intelligence-driven security* as well as *prescriptive security* that looks at both (a) *potential and probability*, and (b) *assigns resources disproportionally to the "unknown" than it does to the "known*." In open societies, especially where the public is invited to engage in a wide range of activities including commercial activity, degrees of risk will always be present when balancing security needs against convenience and the freedom to operate. Therefore, no program can be 100 percent secure, and each airport and situation will be unique, requiring its own assessment and mitigation processes. It is up to policy makers and airport management to decide how limited resources will be allocated in securing the airport while continuing to operate as a public facility.

0	1	2	3	4	5
NOT APPLICABLE	NO PREPAREDNESS	SOME PREPAREDNESS	PREPARED	WELL PREPARED	FULLY PREPARED

[YEAR] AIRPORT SECURITY ASSESSMENT

0	1	2	3	4	5
NOT APPLICABLE	NO PREPAREDNESS	SOME PREPAREDNESS	PREPARED	WELL PREPARED	FULLY PREPARED

	Pre-Event	Event	Event	Post-Event	Mitigation
TOPIC	**PREPAREDNESS**	**DETECT**	**RESPOND**	**RECOVER**	**COMMENTS**
1. AIRPORT SECURITY PLAN					
a. Record of revisions					
b. Table of Contents					
c. Emergency Phone Numbers					
d. Disclosure Statement and Responsibilities					
e. General Information (for example, Foreword, Introduction and Purpose, Distribution, Name & Location, Airport Activities, Airport Description					
f. Definitions & Terms					
g. Administration					
h. Aircraft Movement Areas					
i. Airport Security Procedures					
j. Airport Emergency Grid Map					
k. Identification of Airport Personnel (Incl. TSA GA inspections)					
l. Identification of Vehicles					
m. Law Enforcement & ARFF					
n. Special Event (Incl. National Security Events)					
o. Increased Security Threats					
p. Airport Watch Program					
q. Reward & Feedback Program					
r. Aviation Security Contingency Plans (Incl. Lockdown Procedures, Crisis Counseling)					
s. Airport Continuity of Operations Plan					

[YEAR] AIRPORT SECURITY ASSESSMENT

0	1	2	3	4	5
NOT APPLICABLE	NO PREPAREDNESS	SOME PREPAREDNESS	PREPARED	WELL PREPARED	FULLY PREPARED

	Pre-Event	**Event**	**Event**	**Post-Event**	**Mitigation**
TOPIC	**PREPAREDNESS**	**DETECT**	**RESPOND**	**RECOVER**	**COMMENTS**
t. Exhibits (for example, Airport Emergency Grid Map, Airport Tenant Map, Airport Layout Plan, Bomb Threat Card, Government & Industry Actions, Bomb Blast Stand-off Card, FBO report card, GA Alert Check List)					
u. Other					
2. AIRPORT EMERGENCY PLAN					
a. Record of Revisions					
b. Table of Contents					
c. Emergency Phone Numbers					
d. Definitions & Terms					
e. Preface					
f. Participating Agencies					
g. Assignment of Duties & Responsibilities					
h. Emergency Communications					
i. Crowd Control					
j. Medical Services					
k. Family & Victim Assistance					
l. Public Information					
m. Types of Emergencies & Response Procedures (Alert I, Alert II, Alert III, Structural Fires/Incidents, Severe Storms, Bomb Threats, Sabotage, Hijacking, Power Failures)					

[YEAR] AIRPORT SECURITY ASSESSMENT

0	1	2	3	4	5
NOT APPLICABLE	NO PREPAREDNESS	SOME PREPAREDNESS	PREPARED	WELL PREPARED	FULLY PREPARED

	Pre-Event	**Event**	**Event**	**Post-Event**	**Mitigation**
TOPIC	**PREPAREDNESS**	**DETECT**	**RESPOND**	**RECOVER**	**COMMENTS**
n. Exhibits (Emergency Grid Map, Tenant Address Map, Aircraft Operating Areas, Emergency Staging Areas, Fuel Farm Map, Evacuation Plan, Lockdown Plan, Call Down List, Bomb Threat Card, Suspicious Package Recognition & Handling Plan, ATCT "Zero" Procedure, HazMat Contractor List)					
o. Business Continuity Plan					
p. Other					
3. ACCESS CONTROLS					
a. Controlled entrances (for example, doors, entryways, gates, turnstiles, door alarms)					
b. Control of Materials (for example, , fuel, other)					
c. Secure perimeter (for example, fences, bollards)					
d. Restricted access areas (for example, key assets, roofs, HVAC, fuel farms, electrical vaults)					
e. Access identification (for example, employee badges, biometrics, etc.)					
f. Signage					
g. CCTV					
h. Other					

Warning. This record contains Sensitive Security Information ("SSI") that is controlled under 49 Code of Federal Regulations ("CFR"), Parts 15 and 1520. No part of this record may be disclosed to persons without a "need to know" as defined in 49 CFR 15 and 1520, except with the written permission from the Administrator of the Transportation Security Administration. Unauthorized release may result in civil penalty or other action. For U.S. government agencies, public disclosure is governed by 5 U.S.C. 552 and 49 CFR 15 and 1520.

[YEAR] AIRPORT SECURITY ASSESSMENT

0	1	2	3	4	5
NOT APPLICABLE	NO PREPAREDNESS	SOME PREPAREDNESS	PREPARED	WELL PREPARED	FULLY PREPARED

	Pre-Event	Event	Event	Post-Event	Mitigation
TOPIC	**PREPAREDNESS**	**DETECT**	**RESPOND**	**RECOVER**	**COMMENTS**

[YEAR] AIRPORT SECURITY ASSESSMENT

0	1	2	3	4	5
NOT APPLICABLE	NO PREPAREDNESS	SOME PREPAREDNESS	PREPARED	WELL PREPARED	FULLY PREPARED

	Pre-Event	Event	Event	Post-Event	Mitigation
TOPIC	**PREPAREDNESS**	**DETECT**	**RESPOND**	**RECOVER**	**COMMENTS**
4. BARRIERS					
a. Walls, earth banks & berms (blast protection)					
b. Fences (for example, barbed wire, chain link)					
c. Screens & shields (for example, visual screening)					
d. Vehicle barriers (for example, bollards, jersey barriers, planters, vehicles used as temporary barriers)					
e. Other					
5. MONITORING & SURVEILLANCE					
a. CCTV (for example, fixed, pan, IR, Thermal)					
b. Motion Detectors					
c. Fire & Carbon Monoxide Detectors					
d. Explosive Detectors					
e. Chemical Agent Detectors					
f. Biological Agent Detectors					
g. Radiological Agent Detectors					
h. Metal Detectors					
i. Night-vision Optics (IR, thermal)					
j. Lighting (for example, buildings, perimeter)					
k. Other					

Warning. This record contains Sensitive Security Information ("SSI") that is controlled under 49 Code of Federal Regulations ("CFR"), Parts 15 and 1520. No part of this record may be disclosed to persons without a "need to know" as defined in 49 CFR 15 and 1520, except with the written permission from the Administrator of the Transportation Security Administration. Unauthorized release may result in civil penalty or other action. For U.S. government agencies, public disclosure is governed by 5 U.S.C. 552 and 49 CFR 15 and 1520.

[YEAR] AIRPORT SECURITY ASSESSMENT

0	1	2	3	4	5
NOT APPLICABLE	NO PREPAREDNESS	SOME PREPAREDNESS	PREPARED	WELL PREPARED	FULLY PREPARED

	Pre-Event	**Event**	**Event**	**Post-Event**	**Mitigation**
TOPIC	**PREPAREDNESS**	**DETECT**	**RESPOND**	**RECOVER**	**COMMENTS**
6. COMMUNICATIONS					
a. Telephone (for example, land line, mobile, satellite)					
b. Radios (for example, 800 MHZ, VHF, UHF, battery/hand-powered)					
c. Interoperable Equipment (W/ other agencies)					
d. Redundant & Backup Communications Capabilities					
e. Data Lines (for example, internet, perimeter, permanent, temporary, solar/wind powered)					
f. Other					
7. INSPECTION					
a. Check Points (strategic locations, guard shack, etc.					
b. Personnel Searches (for example, employees, visitors, contractors, vendors)					
c. Vehicle searches (for example, cars, trucks)					
d. Aircraft searches (based & transient)					
e. Hangar searches (private, FBO, SASO)					
f. Building searches (all)					
g. Cargo & Shipment searches					

[YEAR] AIRPORT SECURITY ASSESSMENT

0	1	2	3	4	5
NOT APPLICABLE	NO PREPAREDNESS	SOME PREPAREDNESS	PREPARED	WELL PREPARED	FULLY PREPARED

	Pre-Event	Event	Event	Post-Event	Mitigation
TOPIC	**PREPAREDNESS**	**DETECT**	**RESPOND**	**RECOVER**	**COMMENTS**
h. X-ray Screening (or known shipper)					
i. Other					
8. SECURITY FORCE(S)					
a. Force Size & Jurisdiction					
b. Equipment (weapons, communications, vehicles, SWAT, specialized incident response gear [CBRNE], etc.)					
c. Training					
d. SOP & Special Operating Procedures (patrols, checkpoints, LE including Local, State and Federal, incl. IGA & LOA, mutual aid agreements)					
e. Coordination among security/response teams (NIMS Training)					
f. Other					
9. CYBER SECURITY					
a. Firewalls (VPN, etc.)					
b. Virus Protection					
c. Password Procedures					
d. Information Encryption					
e. Computer Access Control					
f. Intrusion Detection					
g. Redundant & Back Up Systems					
h. Hosted Sites					

Warning. This record contains Sensitive Security Information ("SSI") that is controlled under 49 Code of Federal Regulations ("CFR"), Parts 15 and 1520. No part of this record may be disclosed to persons without a "need to know" as defined in 49 CFR 15 and 1520, except with the written permission from the Administrator of the Transportation Security Administration. Unauthorized release may result in civil penalty or other action. For U.S. government agencies, public disclosure is governed by 5 U.S.C. 552 and 49 CFR 15 and 1520.

[YEAR] AIRPORT SECURITY ASSESSMENT

0	1	2	3	4	5
NOT APPLICABLE	NO PREPAREDNESS	SOME PREPAREDNESS	PREPARED	WELL PREPARED	FULLY PREPARED

	Pre-Event	Event	Event	Post-Event	Mitigation
TOPIC	PREPAREDNESS	DETECT	RESPOND	RECOVER	COMMENTS
i. Third Party Assessment					
j. Other					
10. SECURITY PROGRAM					
a. Employee Background Checks					
b. Tenant Background Checks					
c. Alternative Background Vetting (RBS)					
d. Visitor Control & Monitoring					
e. Foreign Visitor Security Protocol (for example, FBI)					
f. Security Reporting System					
g. Operations Security Plan (See #2)					
h. Coordination among FBOs, SASOs, tenants & Local, State and Federal Law Enforcement					
i. Other					
11. INCIDENT RESPONSE					
a. Emergency Response Plan					
b. Emergency Response Equipment					
c. Emergency Response Personnel					
d. Emergency Response Training, drills & TTXs					
e. Shelter Facilities					
f. Evacuation Procedures					
g. Communications Internal/External					
h. NIMS					

Warning. This record contains Sensitive Security Information ("SSI") that is controlled under 49 Code of Federal Regulations ("CFR"), Parts 15 and 1520. No part of this record may be disclosed to persons without a "need to know" as defined in 49 CFR 15 and 1520, except with the written permission from the Administrator of the Transportation Security Administration. Unauthorized release may result in civil penalty or other action. For U.S. government agencies, public disclosure is governed by 5 U.S.C. 552 and 49 CFR 15 and 1520.

[YEAR] AIRPORT SECURITY ASSESSMENT

0	1	2	3	4	5
NOT APPLICABLE	NO PREPAREDNESS	SOME PREPAREDNESS	PREPARED	WELL PREPARED	FULLY PREPARED

	Pre-Event	Event	Event	Post-Event	Mitigation
TOPIC	**PREPAREDNESS**	**DETECT**	**RESPOND**	**RECOVER**	**COMMENTS**
i. Other					

Warning. This record contains Sensitive Security Information ("SSI") that is controlled under 49 Code of Federal Regulations ("CFR"), Parts 15 and 1520. No part of this record may be disclosed to persons without a "need to know" as defined in 49 CFR 15 and 1520, except with the written permission from the Administrator of the Transportation Security Administration. Unauthorized release may result in civil penalty or other action. For U.S. government agencies, public disclosure is governed by 5 U.S.C. 552 and 49 CFR 15 and 1520.

[YEAR] AIRPORT SECURITY ASSESSMENT

0	1	2	3	4	5
NOT APPLICABLE	NO PREPAREDNESS	SOME PREPAREDNESS	PREPARED	WELL PREPARED	FULLY PREPARED

	Pre-Event	Event	Event	Post-Event	Mitigation
TOPIC	**PREPAREDNESS**	**DETECT**	**RESPOND**	**RECOVER**	**COMMENTS**
12. PERSONNEL PROTECTION					
a. Protection for High-value targets (for example, elected officials, tenants, alternative ingress/egress points)					
b. Protection for Employees (for example, Alerts, reduced travel, asymmetric schedules, shelter, personnel protective equipment/PPE)					
c. Other					
13. INFRASTRUCTURE INTERDEPENDENCIES					
a. Electrical Vaults/Grid (for example, generators, conduit, etc.)					
b. Backup Generator(s)					
c. Fuel Farms					
d. Pipe Lines					
e. Water Supply					
f. Petroleum Supply					
g. Fiber Optics, T1, DSL Lines					
h. Wireless					
i. Telecommunications					
j. Surveillance (Incl. radar)					
k. ASOS/ATIS					
l. Other					
14. OTHER					
a. RESERVED					

Warning. This record contains Sensitive Security Information ("SSI") that is controlled under 49 Code of Federal Regulations ("CFR"), Parts 15 and 1520. No part of this record may be disclosed to persons without a "need to know" as defined in 49 CFR 15 and 1520, except with the written permission from the Administrator of the Transportation Security Administration. Unauthorized release may result in civil penalty or other action. For U.S. government agencies, public disclosure is governed by 5 U.S.C. 552 and 49 CFR 15 and 1520.

[YEAR] AIRPORT SECURITY ASSESSMENT

0	1	2	3	4	5
NOT APPLICABLE	NO PREPAREDNESS	SOME PREPAREDNESS	PREPARED	WELL PREPARED	FULLY PREPARED

	Pre-Event	Event	Event	Post-Event	Mitigation
TOPIC	**PREPAREDNESS**	**DETECT**	**RESPOND**	**RECOVER**	**COMMENTS**

APPENDIX B – AIRPORT SECURITY PROGRAM TEMPLATE

[Airport Name]

GA Airport Security Program

(Original Publication Date) (Date Last Revised)

Table of Contents

Outline all 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 made to those who have an operational need to know, and restricted from all others.

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
(For example, 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 personnel with security related responsibilities
- Individual tenants with specific security related roles

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 (for example, 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 (for example, FSD, alternate contacts).

- All Emergencies 9-1-1
- 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 and acronyms to enhance clarity within the document.

Section IV: Administration

1. Airport Operator: List who operates the airport.

2. Individual who is responsible for airport security

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

- Complete list of security measures.
- 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 Program.
- Maintaining and updating the Airport Security Program to reflect the current state of conditions at the airport.
- Timely distribution of the Airport Security Program 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.

APPENDIX C – BOMB THREAT CALL CHECKLIST

Fill out completely, immediately after bomb threat and **call 9-1-1**

1. Exact wording of the threat:

2. Questions to ask:
   a. When is the bomb going to explode?
   b. What kind of bomb is it?
   c. Where is it right now?
   d. What will cause it to explode?
   e. Why?
   f. Where are you now?
   g. What is your name?
   h. What is your address?

3. Describe the caller:
   a. Sex
   b. Age
   c. Race
   d. Voice (circle all that apply)
      1. Calm
      2. Laughing
      3. Lisp
      4. Disguised
      5. Angry
      6. Crying
      7. Raspy
      8. Accent
      9. Excited
      10. Normal
      11. Deep
      12. Slow
      13. Ragged
      14. Slurred
      15. Nasal
      16. Soft
      17. Loud
      18. Stutter
      19. Clearing throat
      20. Deep breathing
      21. Cracking voice
      22. Other (describe)
   e. If the caller's voice was familiar, who did it sound like?

4. Background Noises
   a. Street
   b. House
   c. Factory
   d. Motor
   e. Machinery
   f. Long distance
   g. Voices
   h. Office
   i. Animals
   j. Clear
   k. Music
   l. Static
   m. P.A. system
   n. Other (describe)

5. Threat language (circle all that apply):
   a. Well spoken
   b. Educated
   c. Sober
   d. Incoherent
   e. Irrational
   f. Intoxicated
   g. Foul

6. Was the threat delivered/communicated by the caller, or a recorded message?

7. Please indicate any additional remarks:

8. Full name of person who received the call:
   a. Job title:
   b. Telephone number:

APPENDIX D – 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 version 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 web site at www.faa.gov]

00-2, *Advisory Circular Checklist* - Contains a listing of all current advisory circulars.
150/5200-31A, Airport Emergency Plan
150/5300-13, Airport Design
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.
150/5370-10, Standards for Specifying Construction of Airports

Establishment of the Department of Homeland Security, Transportation Security Administration
On November 19, 2001, Congress enacted the Aviation and Transportation Security Act (ATSA), Public Law 107–71, 115 Stat. 597, which established TSA. Pursuant to ATSA, 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 Title 49 of the Code of Federal Regulations.

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).[15] The following regulations apply to regulated aviation entities, not necessarily to GA operators or facilities, and are provided for reference and informational purposes only.

- **Part 15,** *Protection of Sensitive Security Information* - This part governs the maintenance, safeguarding, and disclosure of records and information that the Secretary of DOT has determined to be Sensitive Security Information, as defined in § 15.5. This part does not apply to the maintenance, safeguarding, or disclosure of classified national security information, as defined by Executive Order 12968, or to other sensitive unclassified information that is not SSI, but that nonetheless may be exempt from public disclosure under the Freedom of Information Act. In addition, in the case of information that has been designated as critical infrastructure information under section 214 of the Homeland Security Act, the receipt, maintenance, or disclosure of such information by a

[15] Many TSRs are former rules of the Federal Aviation Administration (FAA) that were transferred to TSA when TSA assumed FAA's civil aviation security functions on February 17, 2002 (67 FR 7939; February 20, 2002).

Federal agency or employee is governed by section 214 and any implementing regulations, not by this part.

- **Part 1520,** *Protection of Sensitive Security Information* - This part governs the maintenance, safeguarding, and disclosure of records and information that TSA has determined to be Sensitive Security Information, as defined in § 1520.5. This part does not apply to the maintenance, safeguarding, or disclosure of classified national security information, as defined by Executive Order 12968, or to other sensitive unclassified information that is not SSI, but that nonetheless may be exempt from public disclosure under the Freedom of Information Act. In addition, in the case of information that has been designated as critical infrastructure information under section 214 of the Homeland Security Act, the receipt, maintenance, or disclosure of such information by a Federal agency or employee is governed by section 214 and any implementing regulations, not by this part.

- **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 rules that apply to persons engaged in aviation-related activities, including passengers, aviation employees, airport operators, aircraft operators, foreign air carriers, and others.

- **Part 1542,** *Airport Security* - This part requires airport operators regularly serving U.S. and foreign passenger air carriers 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 individuals seeking unescorted access authority at a regulated airport. This part also describes the requirements related to Security Directives issued to airport operators. This part also provides that TSA may enter and be present at an airport that does not have a security program under this part, without access media or identification media issued or approved by an airport operator or aircraft operator, to inspect an aircraft operator operating under a security program under part 1544 of this chapter, or a foreign air carrier operating under a security program under part 1546 of this chapter. 49 CFR 1542.5(e).

- **Part 1544,** *Aircraft Operator Security: Air Carriers and Commercial Operators* - This part applies to certain aircraft operators holding operating certificates for certain scheduled passenger operations, public charter passenger operations, private charter passenger operations, all-cargo operations, and certain 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, and fingerprint-based criminal history record checks for flightcrew members and those with unescorted access authority. This part also describes requirements applicable to law enforcement officers flying armed aboard an aircraft. This part describes the requirements related to Security Directives issued to aircraft operators.

- **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, Subchapter B – Security Rules for All Modes of Transportation.

- **1552,** *Flight Schools* - This subpart applies to flight schools that provide instruction under 49 U.S.C. Subtitle VII, Part A, in the operation of aircraft or aircraft simulators, and individuals who apply to obtain such instruction or who receive such instruction.

- **Part 1554,** *Aircraft Repair Station Security* - This part applies to repair stations and requires repair stations certificated under 14 CFR Part 145 to allow TSA and DHS officials to enter, conduct inspections, and view and copy records as needed to carry out TSA's security-related statutory and regulatory responsibilities. The regulation also requires these repair stations to comply with security directives when issued by the TSA. The regulation also requires certain repair stations to implement a limited number of security measures.

- **1562,** *Operations in the Washington, DC, Metropolitan Area* - This subpart applies to the following airports, and individuals who operate an aircraft to or from those airports, that are located within the airspace designated as the Washington, DC, Metropolitan Area Flight Restricted Zone by the Federal Aviation Administration: 1) College Park Airport (CGS); 2) Potomac Airfield (VKX); and Washington Executive/Hyde Field (W32).

TSA, DOD, DOS, FEMA and other reports

1. U.S. Department of Homeland Security, Transportation Security Administration*, TSA Recommended Security Guidelines for Airport Planning, Design and Construction*, May 2011

2. TSA Aviation Security Advisory Committee, *Report of the GA Airports Security Working Group,* October 1, 2003.

3. American Association of Airport Executives, *GA Airport Security Task Force Recommendations,* June 2002.

4. National Association of State Aviation Officials, *General Aviation*, December 2002.

5. U. S. Department of Defense: UFC 4-010-01 United Facilities Criteria, DOD Minimum Antiterrorism Standards for Buildings, February 2012; and Change 1, October 2013.

6. U.S. Department of State: SD-STD-02.01, Test Method for Vehicle Crash Gate Testing of Perimeter Barriers and Gates, Revision A, March 2003.

7. FEMA Publications
    - FEMA 426 - Reference Manual to Mitigate Potential Terrorist Attacks Against Buildings, 2nd Edition (2011)
    - FEMA 427 - Primer for Design of Commercial Buildings to Mitigate Terrorist Attacks (2003)
    - FEMA 429 - Insurance, Finance, and Regulation Primer for Terrorism Risk Management in Buildings (2002)
    - FEMA 430 - Site and Urban Design for Security: Guidance Against Potential Terrorist Attacks (2007)
    - FEMA 455 - Handbook for Rapid Visual Screening of Buildings to Evaluate Terrorism Risks (2009)

8. Chain Link Fence Industry Publications
    - Chain Link fence manufacturer's Institute (CLFMI) at www.chainlinkinfo.org
    - Chain Link Fence Manufacturers Institute, Chain Link Fence Wind Load Guide for the Selection of Line Post and Line Post Spacing (WLG 2445), Revised 2012
    - Chain Link Fence Manufacturers Institute Security Fencing Recommendations (CLF-SFR0111)
    - Chain Link Fence Manufacturers Institute Product Manual, CLF-PM0610, (revised January, 2012)
    - American Society for Testing and Materials (ASTM)
        - F 567 - Standard Practice for Installation of Chain-Link Fence
        - F 2611 - Standard Guide for Design and Construction of Chain Link Security Fencing
        - F 900 - Specification for Industrial and Commercial Swing Gates
        - F 2200 - Specification for Automated Vehicular Gate Construction

9. Airport Cooperative Research Program, *General Aviation Safety and Security Practices* (2007)

10. U.S. Government Accountability Office (GAO), *General Aviation Security Assessments at Selected Airports* (May 2011)

APPENDIX E – USEFUL WEBSITES AND CONTACTS

Aviation trade associations

Organization	Website
Aircraft Owners and Pilots Association	www.aopa.org
Airports Council International – North America	www.aci-na.org
Airport 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 Aviation Association	www.agaviation.org
National Air Transportation Association	www.nata.aero
National Association of State Aviation Officials	www.nasao.org
National Business Aviation Association	www.nbaa.org
United States Parachute Association	www.uspa.org
National Association of Flight Instructors	www.nafinet.org

Federal government

Organization	Website
Department of Homeland Security	www.dhs.gov
Department of Homeland Security – Blue Campaign	www.dhs.gov/blue-campaign
Federal Aviation Administration	www.faa.gov
Federal Bureau of Investigation	www.fbi.gov
Transportation Security Administration	www.tsa.gov

FAA Regional Operations Centers

Facility Region	States Covered	Phone Number	Email Address
Western ROC	AK, AZ, CA, CO, HI, ID, MT, NV, OR, UT, WA, WY	425-227-1999	9-WSA-OPSCTR@faa.gov
Central ROC	AR, IA, IL, IN, KS, LA, MI, MN, MO, ND, NE, NM, OH, OK, SD, TX, WI	817-222-5006	9-CSA-ROC@faa.gov

East ROC	AL, CT, FL, GA, KY, MA, ME, MS, NC, NH, PR, RI, SC, TN, VI, VT	404-305-5180	9-ASO-ROC@faa.gov
East ROC	DC, DE, MD, NJ, NY, PA, VA, WV	404-305-5150	7-AEA-ROC@faa.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	www.chainlinkinfo.org