DEDICATED TO HELPING BUSINESS ACHIEVE ITS HIGHEST GOALS.

NBAA

BEST PRACTICES FOR BUSINESS AVIATION SECURITY

Best Practices for Business Aviation Security

Aviation security has become the responsibility of individuals and organizations across the aviation industry – from ground crews and schedulers, to pilots, business leaders and government officials. NBAA seeks to assist industry and regulatory standard setting bodies (DHS, TSA, FAA, ICAO) in developing security guidelines that recognize the unique characteristics of business aviation. NBAA members are urged to review these best practices to help ensure the best possible security for the business aviation operator, both at and away from their home base.

ASSESS YOUR RISK

The first step in the development of an effective security program is to assess the threat level against the operator (including its personnel, aircraft and facilities) and the operator's vulnerabilities. Threats may relate to the nature of business the organization conducts, where that business is conducted, the nationality of the organization and/or aircraft, the profile of its passengers and the value of goods carried.

Information on the various kinds of threats the operator is subject to will come from a variety of sources. In developing and maintaining a current threat assessment for areas of operations, the manager should use the following resources as appropriate:

- National and local security officials
- National and local law enforcement officials
- National and international trade associations
- Air security assessment and intelligence service providers
- The organization's security officer, if applicable
- Organization officials posted in foreign locations, if applicable
- U.S. Department of State and Overseas Security Advisory Council
    - www.travel.state.gov
    - www.osac.gov

Security professionals can provide assistance in determining and assessing the operator's vulnerabilities. Once an operator has determined their own risk profile, each operator should develop best practices to mitigate those specific risks, publish those practices for personnel use, implement the practices and train their personnel accordingly.

The following best practices are recommended.

STRATEGIC PLANNING

In the present threat environment, the private sector remains the first line of defense for its own assets and facilities. Companies have the most incentive to invest in security and are often in the best position to determine the immediacy of security concerns. Additionally, they are better able to assess the magnitude of security concerns and to devise effective responses. The following steps should be taken in developing and maintaining any security plan.

- Maintain frequent contact with the company's security department; information gathered on aircraft and flightcrew security should be shared with the security department
- Consider removal of company identification, logos and the American flag insignia
- Refrain from making controversial statements, either in public or in private
- Be sensitive to security information received just before flight time
- Demonstrate caution when conducting aircraft transactions – for example, be wary of any last-minute changes to fund transfer instructions, fraudulent emails and other indications of possible fraud

Once the security program is in place, it is critical to refine and test the plan with tabletop, simulated incident or enterprise exercises.

People

FLIGHT DEPARTMENT PERSONNEL

- Establish and maintain a communications link with the company security department or the equivalent
    - Communicate security needs to top management
- Establish a security manager position
- Complete annual security training
- Conduct background checks of flight department personnel
    - Credit
    - Employment
    - Professional credentials
    - Criminal history background check, when possible
    - Flight department personnel background checks should be updated no less frequently than every five years for employees and every two years for contract personnel
- Be alert for troubled personnel
    - Company personnel will remain diligent to changes in emotional well-being and health of all crewmembers and ground personnel; crewmembers and ground personnel that are considered to be a risk to the safety or security of a flight should be removed from duty (14 CFR 61.53)

PASSENGERS

- Confirm the identity and authority of passengers
- Be alert for troubled passengers
    - Company personnel will remain diligent to changes in emotional well-being and health of all passengers; passengers that are considered to be a risk to the safety or security of a flight should not be allowed to board the aircraft
- Firearms or other weapons must be handled strictly in accordance with company policy

Facilities

HOME BASE: OPERATOR-CONTROLLED

- Ensure home facility perimeter security
- All street-side gates and doors are to be closed and locked at all times
- Require positive access control for all external gates and doors
- Close and lock hangar doors when unattended
- Activate hangar security system when unattended
- Secure all key storage areas (food & liquor, parts & tools, etc.) when unattended
- Have an access control management system for keys and electronic passes
- Confirm passengers' identity and authority prior to allowing access to facilities and aircraft
- Escort all visitors on the ramp and in the hangar area
- Use a government issued photo ID to verify identity of any visitor or vendor
- Post emergency numbers prominently around facility
- Ensure easy access to phones or panic buttons in various locations (break room, hangar bay, visitor lounge, etc.)
- Be aware of your surroundings and do not be complacent – challenge strangers to provide identification and purpose of visit

- If in doubt, deny access
- Outdoor signage should be prominently displayed near areas of general public access warning against tampering with aircraft or unauthorized use of aircraft

HOME BASE: TENANT FACILITY

- Comply with security measures of tenant facility
- Be aware of facility emergency contact numbers
- Confirm passengers' identity and authority prior to allowing access to aircraft
- Use a government issued ID to verify identity of any operator visitor or vendor
- Escort all operator visitors on the ramp and in the hangar area
- Be aware of your surroundings and do not be complacent
- If in doubt, advise tenant facility staff.

TRANSIENT FACILITY

The flight department (i.e., scheduler, flightcrew, etc.) must ensure security measures at destination FBOs are consistent with or exceed home base facility security measures described above. If destination security measures are insufficient, the flightcrew should consider repositioning the aircraft or supplementing the level of security to achieve the appropriate security environment.

Aircraft

PREFLIGHT

- All flight crewmembers must wear photo ID
- A flight crewmember (or other authorized personnel) must be present at all times when the aircraft is being serviced (fueling, catering, etc.)
- An aircraft physical security inspection should be conducted following any servicing of the aircraft
- An aircraft physical security inspection should be conducted prior to every flight in order to verify that there are no suspicious items on board the aircraft. At a minimum, the inspection must include the following areas:
    - Externally accessible service compartments that do not require the use of tools or special equipment to gain access
    - Wheel wells
    - System openings and vents
    - Lavatories
    - Internal and external storage compartments
    - Baggage holds
    - Mechanical and electronic compartments that do not require the use of tools or special equipment to gain access
- If the aircraft physical security inspection identifies any suspicious items, the crew will not attempt to remove the object and will immediately notify nearest local law enforcement official
- Once found to be secure, crewmember remains with aircraft, or it is locked then unattended aircraft procedures are enacted
- Require an accurate and accessible passenger manifest for all trip legs
- Positively match passengers to that manifest by either:
    1. A government issued identification containing a picture, expiration date, name and date of birth, or
    2. Verification of identification by known passenger

    (Note: This check does not apply to children under 15 years of age)

- Any luggage not matched with a passenger or aircraft crewmember will not be placed on board the aircraft
    - The crew may allow unaccompanied company material on board the aircraft only if the material has been inspected for suspicious items; if any objects are found, the crew will immediately notify local law enforcement officials for further inspection

AIRCRAFT

Use appropriate security equipment, including (as applicable):

- Door locks
- Throttle locks
- Propeller locks
- Other security or surveillance equipment

UNATTENDED AIRCRAFT

- Any unattended aircraft is to be secured in such a manner as to prevent unauthorized entry
    - Utilize aircraft flight manual recommendations if available
    - Close and secure emergency exits
    - Arm alarm systems, if installed
    - Close and lock all keyed access doors
    - Utilize operator specific procedures for your aircraft
- A system will be utilized to detect unauthorized entry into the aircraft and external openings.
    - A system can be, but is not limited to, electronic security alarm and notification systems, security tape, closed circuit television with continuous monitoring, guards, etc.
    - If unauthorized entry is suspected, the crew will notify nearest law enforcement official.
- Security for unattended aircraft varies based on the scenario:
    - Unattended aircraft parked in hangar with controlled access
    - Unattended aircraft parked on ramp with all keyed access doors closed and locked
    - Unattended aircraft parked on ramp using alternative means of compliance such as, but not limited to:
        - Hardened throttle/quadrant lock
        - Aviation security tape (“tamper tape”)
        - Prop locks for piston aircraft
        - Tie-down lock(s)

Procedures

INFORMATION

- All oral and written flight information should be distributed on a need-to-know basis
- Any paper documents that could compromise the security of future operations (flight schedule, passenger manifests, contact information, etc.) should be destroyed after use, except where required by corporate policy or governmental regulation (i.e. CFRs)
- Department personnel should only discuss schedules or flight details with others on a need-to-know basis

FLIGHT PLANNING

- Receive a destination intelligence briefing
- Assess each destination security risk for travelers: high, significant, medium, low
- Review all sources of media information; newspaper, radio and television coverage of actual events can be very instructive, especially prior to visiting a new destination
- Review duress communication procedures and security related emergency procedures (bomb threat, hijacking/terrorist acts, intercept procedures etc.)
- Use the aircraft's security system at every stop, no matter how brief
- Be very cautious when hiring local guards; local contacts can assist in making arrangements for theft
- Establish an approved vendor (catering, transport, FBO, etc.) list based on standardize vetting processes.
- Review the current National Terrorism Advisory System (NTAS) status

CYBER SECURITY

- Assess the level of risk for the aircraft and mobile devises based on location and operation
- Develop formal policies regarding the use, storage and sharing of flight department data that mitigate the risks of hacking or corruption
- Establish best practices for device usage, especially away from the home network (i.e. international travel, etc.)
- Protect aircraft identification information by prohibiting public distribution of aircraft photos, registration information and other identifying features
- Block your aircraft tail number using the BARR program
- Publish social media usage and network policies that mitigate the risk of sensitive data leaking from the organization

TRAINING

- Conduct initial and annual security training, including emergency response training, for all flight department personnel
- Require frequent passengers to complete basic security training on topics including aircraft, cyber, facility and personal security, especially for international travel
    - This should include basic security response training

SECURITY BREACH RESPONSE PLANNING

NBAA recommends that aviation departments consider the following steps in developing a company security program:

- Establish an emergency control committee to handle disaster-type emergencies
- Develop a contingency plan for advance response to hijackings, bomb threats, executive abductions, terrorist activities and extortion demands
- Schedule simulated emergencies at least once a year to test the contingency plan
- Establish an emergency communication system with a telephone list of key personnel
- Report security breaches to the TSA's Transportation Security Operations Center (TSOC) by calling 703-563-3240 or 877-456-8722

National Business Aviation Association
1200 G Street NW, Suite 1100
Washington, DC 20005
www.nbaa.org
(202) 783-9250 | ops@nbaa.org

ACKNOWLEDGMENTS

NBAA thanks the volunteers of its Security Council for developing these best practices for business aviation security.

ABOUT NBAA

Founded in 1947 and based in Washington, DC, the National Business Aviation Association (NBAA) is the leading organization for companies that rely on general aviation aircraft to help make their businesses more efficient, productive and successful. Contact NBAA at 800-FYI-NBAA or info@nbaa.org. Not a member? Join today by visiting www.nbaa.org/join.