

Airport Security Department
Airport ID Processing Center

Westchester County Airport

– Signatory Authority Training –

Revision: 05-2015

SENSITIVE SECURITY INFORMATION

WARNING: THIS RECORD CONTAINS SENSITIVE SECURITY INFORMATION THAT IS CONTROLLED UNDER 49 C.F.R. PARTS 15 AND 1520. NO PART OF THIS RECORD MAY BE DISCLOSED TO PERSONS WITHOUT A "NEED TO KNOW," AS DEFINED IN 49 C.F.R. PARTS 15 AND 1520, EXCEPT WITH THE WRITTEN PERMISSION OF THE ADMINISTRATOR OF THE TRANSPORTATION SECURITY ADMINISTRATION OR THE SECRETARY OF TRANSPORTATION. UNAUTHORIZED RELEASE MAY RESULT IN CIVIL PENALTIES OR OTHER ACTION. FOR U.S. GOVERNMENT AGENCIES, PUBLIC DISCLOSURE GOVERNED BY 5 U.S.C. 552 AND 49 C.F.R. PARTS 15 AND 1520.

Introduction

Understanding the background for having Signatory Authorities

Transportation Security Administration mandates commercial service airports, which have an ID badging system in place to identify and train “Signatory Authorities”. Westchester County Airport has chosen the name “Authorized Signer” to describe this group of individuals. Authorized Signers have a crucial role in administering and maintaining the integrity of the Westchester County Airport ID badge program. Authorized Signatory is the individual or designated representative authorized to sponsor individuals and request airport identification media for them.

The TSA performs a thorough Security Threat Assessment (STA) on every individual applying for or holding airport issued identification media at airports with commercial airline service. Verifying a person's identity and work authorization status is essential to completing a STA. All organizations with personnel working at an airport requiring identification media must have designated company employees who are authorized to sign paperwork verifying every one of their workers applying for that identification media are a company employee and has a legitimate, work related need for the ID. Authorized signers also assist by ensuring applicants present the correct required documents to airport badging offices for verification. This training will cover the basic requirements and responsibilities of company employees who are designated as authorized signers. Authorized Signers’ responsibilities are based on Transportation Security Administration (TSA) and Westchester County Airport Rules and Regulations, as well as the HPN Airport Security Program.

Requirements for being an Authorized Signer:

Authorized signer has to:

- Successfully pass the fingerprinting process and criminal history record check (CHRC)*
- Successfully pass the Security Threat Assessment (STA)
- Successfully pass the SIDA course (not mandatory for signers from companies with AOA badges only)
- Be familiar with the badge application initiation procedures and application forms used in this process
- Be familiar with identification (and immigration, if applicable) documents used in badging process
- Know the badge deactivation and retrieval process

**Not applicable for Authorized Signers who do not sign-off on applications needing fingerprinting (SIDA and FBO)*

SENSITIVE SECURITY INFORMATION

WARNING: THIS RECORD CONTAINS SENSITIVE SECURITY INFORMATION THAT IS CONTROLLED UNDER 49 C.F.R. PARTS 15 AND 1520. NO PART OF THIS RECORD MAY BE DISCLOSED TO PERSONS WITHOUT A “NEED TO KNOW,” AS DEFINED IN 49 C.F.R. PARTS 15 AND 1520, EXCEPT WITH THE WRITTEN PERMISSION OF THE ADMINISTRATOR OF THE TRANSPORTATION SECURITY ADMINISTRATION OR THE SECRETARY OF TRANSPORTATION. UNAUTHORIZED RELEASE MAY RESULT IN CIVIL PENALTIES OR OTHER ACTION. FOR U.S. GOVERNMENT AGENCIES, PUBLIC DISCLOSURE GOVERNED BY 5 U.S.C. 552 AND 49 C.F.R. PARTS 15 AND 1520.

- Be aware of the importance of accurately reporting all the changes of status regarding his company and badged employees
- Get re-trained once every 12 calendar months

Responsibilities of the Authorized Signers

Authorized Signers are held responsible for all actions on behalf of his/her company. TSA Regulations and Westchester County Airport policies establish strict standards for the issuance of airport ID cards that provide access to the employees. These standards are defined in TSA Regulation 1542, TSA Security Directives and Airport Security Plan. Authorized Signers administer the program in accordance with these strict standards.

The Authorized Signer manages all aspects of the Westchester County Airport ID Card program for the company that he/she represents. Authorized Signer may also be responsible for badges issued to tenants/subtenants/contractors that the company represented by this authorized signer might sponsor for an airport ID. This includes following:

- 1. Initiation and authorization of airport ID card applications, transactions, individual access, and privileges.**
 - a. Authorized Signers initiate the applications by either enrolling the ID applicant into the SAFE system or signing the ID Authorization Form* for persons that are employees of that company, and are paid directly by the company. The Authorized Signer must verify the identity and work authorization of each employee by personally reviewing required documents detailed on the application. By signing and initialing each application (on paper or electronically), the Authorized Signer verifies this step is completed properly in full compliance with regulations and matches information contained in the United States Citizenship and Immigration Form I-9, completed by the company and included in the employer files.
 - b. Authorized Signers can also execute applications for employees of other companies doing business at Authorized Signer company's premises including subtenants or subcontractors. In this case, along with the ID authorization sheet, an Authorized Signer needs to submit a copy of a notarized letter from subtenant/subcontractor's company confirming completion of the "I-9 process" and eligibility of an applicant for employment in US.
- 2. Updates the Airport Security Department on regular basis, regarding the employee/company information**

SENSITIVE SECURITY INFORMATION

WARNING: THIS RECORD CONTAINS SENSITIVE SECURITY INFORMATION THAT IS CONTROLLED UNDER 49 C.F.R. PARTS 15 AND 1520. NO PART OF THIS RECORD MAY BE DISCLOSED TO PERSONS WITHOUT A "NEED TO KNOW," AS DEFINED IN 49 C.F.R. PARTS 15 AND 1520, EXCEPT WITH THE WRITTEN PERMISSION OF THE ADMINISTRATOR OF THE TRANSPORTATION SECURITY ADMINISTRATION OR THE SECRETARY OF TRANSPORTATION. UNAUTHORIZED RELEASE MAY RESULT IN CIVIL PENALTIES OR OTHER ACTION. FOR U.S. GOVERNMENT AGENCIES, PUBLIC DISCLOSURE GOVERNED BY 5 U.S.C. 552 AND 49 C.F.R. PARTS 15 AND 1520.

This includes the access or escort requirements, employment eligibility or any other changes in status that might affect the airport badge eligibility. This task is accomplished by doing the following:

a. Keeping track of all airport ID badge applications and active badges

Companies are required to keep track of all employees whose airport ID applications were initiated and completed (airport ID badges approved and issued) as well as all incomplete applications (withdrawn or cancelled during the application process). The Authorized Signer must ensure that information about terminated employees is maintained for a period of at least 180 days following termination of the individual's access privileges

b. Accurately reports any changes in employees' statuses

Authorized Signer is responsible of ensuring that only current employees with an operational need to be on the airfield are in possession of an active airport ID. When no longer applicable, the retrieval process must be activated in the following Manner

1. Once an employee has been terminated from employment, an Authorized Signer shall call the Security Department/ID Processing Center or the Airport Operations supervisors **immediately** to inform of such event. This enables the airport personnel to disable the access card immediately to prevent unauthorized entry to secure areas
2. Tenants are responsible for retrieving HPN IDs from their employees at the time of resignation, termination, extended leave of absence, or any other instance where an employer is aware that an employee will not be using the HPN ID for a prolonged period of time. Tenants are responsible for reporting such events to the Airport Security Department immediately
3. If the company operates its own access control system, the facility access must be electronically terminated IMMEDIATELY and airport ID office notified of it.
4. The next step is to email the security department or otherwise make a written notification with an explanation as to why the employee was terminated, or the last time the employee remembers having the ID. This email is to be sent the **day of** the reported loss or termination.
5. ID cards that have been recovered from departing employees (same applies to invalid and expired cards) must be returned into the ID Office ASAP, upon notification to the Airport Security Department that Authorized Signer is in possession of such card
6. For non-recovered cards the company will be denied further processing of any types of airport IDs until a fee for the lost card is paid.
7. Appropriate forms needs to be submitted to the Airport Security department for both recovered ID media, as well as for lost/stolen media
8. When returning the HPN badge of the employee no longer employed at your company to the Airport Security, you are required to use the "ID

SENSITIVE SECURITY INFORMATION

Return/Cancellation Form". It crucial that you indicate on this form that facility badge has been disabled and/or destroyed.

c. Report lost or stolen identification media:

Airport ID media that has been lost, stolen or otherwise not accounted for, jeopardizes the integrity of the airport ID system as a whole. Current TSA regulations mandate replacement of all airport IDs when the percentage of ID cards that are not accounted for reaches 5%. This process carries significant amount of labor and equipment related expenses for the airport operator and a great deal of inconvenience for airport tenants alike.

Lost or stolen identification badges must be reported immediately to the airport operator. To obtain a new badge, the badge holder must complete the Lost ID Replacement Form obtained from Airport Security, and have it signed by an authorized signer from his or her company or facility.

In addition to that, for any lost or stolen ID, there will be a fee assessed to the ID holder. Company takes the responsibility for this fee if the employee leaves without surrendering the airport ID media to the Authorized Signer. Future IDs will not be issued to anyone from that company until either the ID is returned, or the fee is paid (neither to new applicants, nor the existing badge holders seeking the badge renewal).

If the badge is lost or stolen a second time, the employee must re-qualify before a new badge will be issued. If this is a SIDA access badge, the employee must re-take the SIDA Training Course. The Airport still reserves the right to deny the new ID.

A non-refundable fee of \$100.00 is charged for replacement of a lost SIDA ID badge. \$150.00 is charged for replacement of a second lost SIDA ID badge. A third lost ID badge may result in the denial of SIDA access.

A SIDA Visitor ID will not be issued to a SIDA ID holder who forgets his or her ID. They will still be permitted to work, but not within the SIDA area.

SCHEDULE OF FEES FOR LOST or NON-RECOVERED AIRPORT ID MEDIA:

First time loss – \$100.00 (non-refundable)

Second loss – \$150.00 (non-refundable)

Third loss – No more IDs issued

It is a responsibility of the airport ID holder to report the lost or stolen ID media immediately to the Airport Security department. All airport ID card holders have been provided Airport Operations phone number that is active 24/7. It is of uttermost importance to report the loss of SIDA badges immediately. These badges are associated with the airport access control system, and by notifying the Airport Operations or

SENSITIVE SECURITY INFORMATION

Security immediately airport personnel is able to deactivate this card from any possible unauthorized use.

If the loss of airport ID media was reported to the authorized signer, same notification procedures from above must be followed.

d. Respond to Airport ID office audits and training requests:

Airport conducts ID audits as specified in TSA regulations and Airport Security Plan. These audits may include the comprehensive annual audit, quarterly self-audit and unscheduled random audits. Timely response to these audits is mandatory and non-compliance can lead to the “freeze” of all ID activities for the company.

Authorized Signers are required to satisfy the annual recurrent training requirement upon request from the Airport ID office. Airport reserves the right to issue interim training document whenever there is a change in TSA or Airport Security Program requirements.

3. Maintains company’s airport ID cards in accordance with Westchester County Airport and TSA regulations

One of the most important roles of the Authorized Signers is to precisely keep track of all applications for airport badges that he or she authorized. This includes all active badges, but also includes applications for all rejected, abandoned or revoked airport ID badges.

Following the TSA requirements, Westchester County Airport performs (comprehensive and partial) audits of all identification media on a regular basis. These audits include a comparison of the current list of airport-issued identification media holders against the lists maintained by those with signatory authority to identify and resolve any discrepancies.

Authorized Signer must respond to all requests of this kind accurately and within time parameters set up by the Airport Security. The Authorized Signer is required to verify the status of every active Airport ID Card, and ensuring that all non-active Airport ID Cards have been returned or accounted for.

Upon Authorized Signer’s request The Airport Security Department will provide reports with the status of every ID card signed by the Authorized Signer and/or held by his/her company’s employees.

4. Keeps employees informed regarding TSA regulations and airport policies

Important changes to laws, regulations, or policies affecting airport security are communicated to Authorized Signers. The Authorized Signer is an important point of contact between the company and the Airport ID Office. By communicating with the Authorized Signer, the Airport ID Office is able to quickly and efficiently distribute information regarding important changes to TSA Regulations, Westchester County Airport Rules and Regulations. The Authorized Signer is required to communicate changes across

SENSITIVE SECURITY INFORMATION

his/her organization and ensure the company and its employees remain in constant compliance with all requirements.

In order for the Authorized Signer to effectively manage the airport ID processing and maintenance on behalf of the company, and to be able to keep employees informed about regulations the Authorized Signer needs to be familiar with the following components of the airport ID program:

CRIMINAL HISTORY RECORD CHECK (CHRC):

All airport tenants requesting any type of badge for which Criminal History Record Check (CHRC) is one of the requirements (currently SIDA badge and AOA badge with FBO privileges) must do so at the Westchester County Airport ID Office. The results of the CHRC are strictly held between applicants and the Westchester County Airport. An applicant has a right to get a copy of a CHRC results transmitted to the Airport ID Office from the FBI database. The Authorized Signer does not have any access to these results.

Westchester County Airport has discontinued accepting fingerprinting results/CHRCs performed by the TSA-approved air carriers. However, as a courtesy to the customers doing business at HPN the Airport ID office will waive the fingerprinting fee in the amount of \$30, when copy of the CHRC or TSC Case # are submitted along with the ID application.

It is the responsibility of the airport ID applicant to report to the airport and/or Authorized Signer if he/she has any arrests, convictions or any other conditions that might affect the eligibility for an airport ID media. If the Authorized Signer learns about such conditions it is his/her responsibility to notify the Airport ID office immediately.

Applicants must obtain their airport identification media within 30 business days of notification by the airport operator that the applicant passed the STA and the CHRC did not disclose a disqualifying criminal offense.

RE-FINGERPRINTING:

All SIDA and FBO badge holders with more than a 30-day “break in service” as defined by the TSA must be re-fingerprinted. It is the responsibility of the Authorized Signer to ensure every employee is in full compliance with this TSA requirement.

*Break in service – additional clarification:

- Every break in service MUST be communicated to the airport ID office ASAP
- Break in service is judged in two different ways:
 1. Employee transferring from one company based at the HPN to another company based at the HPN
(A key factor here is the official date of employment termination at the previous company.)

SENSITIVE SECURITY INFORMATION

2. Employee on the LOA, unpaid leave, long vacation, etc
(A key factor in judging a break here is the payroll – if the employee is on the payroll all the time, such absence is NOT considered as a break in service even though it is more than 30 days.)

RECURRENT FINGERPRINTING:

Every cardholder who was previously fingerprinted as a part of the airport ID process is subject to recurrent fingerprinting. Recurrent fingerprinting is done at least every two years, usually at the time of airport ID renewal.

SIDA TRAINING AND RE-TRAINING:

SIDA Training is required under TSA regulation prior to any individual being granted access to the SIDA. The course must be conducted in accordance with the curriculum and standards set by the Westchester County Airport and approved by the Transportation Security Administration. The applicant must have completed the course and achieved a satisfactory result on the required testing. Westchester County Airport internal regulations prohibit the attendance at the SIDA course before an applicant has completed all the other requirements for issuing SIDA badge.

The record of SIDA Training is kept at the HPN ID office indefinitely. Returning applicants or employees transferring from another company DO NOT have to take this course again if records of their initial training are still available at the ID office (usually around six months from resigning from the previous employment at the airport). However, the airport ID office strongly encourages such candidates to retake course.

SIDA retraining is required at the time of the SIDA ID renewal. There is no class that ID holders need to attend – it is given in a form of a test covering the most important SIDA security rules.

VALIDITY AND EXPIRATION OF THE AIRPORT ID MEDIA:

Airport ID media are issued for the period of maximum two years from the issue date, set to expire on the ID holder's birthday closer or equal to 2-year mark. It is the responsibility of the ID holder to renew the ID badge before the expiration date. However, the Airport ID processing center will occasionally, send a reminder to the Authorized Signer with a list of airport IDs from that company, which are about to expire in the following weeks/months. In this case, it is the responsibility of the Authorized Signer to communicate this message to all employees. All airport ID badges that are not renewed within 30 days of expiration are reported to the TSA as abandoned and deleted from the airport ID database. In order to re-establish airfield access privileges such individuals are required to surrender the expired badge to the Airport Security, re-apply for the ID and go through the approval process again.

SENSITIVE SECURITY INFORMATION

Additional penalty fees may apply to airport ID holders who fail to renew their airport IDs within 30 days following the expiration date.

Airport ID holders with expired IDs are strictly prohibited from accessing any part of the airfield without proper escort. This includes hangar interiors, which are also considered part of the secure area of the airfield.

SIDA/SECURITY VIOLATIONS:

If the Airport Security issues the Security Violation notice to the employee, the Authorized Signer is the first one to be notified of such occurrence. It is the responsibility of the authorized signer to counsel and/or take disciplinary measures (if necessary) to ensure the employee does not repeat the violation.

If SIDA/AOA ID violation is repeated (2nd time) Authorized Signer must attend the training class and/or counseling session with the Airport Security Personnel together with violator.

TYPES OF AIRPORT ID MEDIA:

It is the responsibility of the authorized signer to determine which type of the airport badge he/she will request for the new employee. Airport ID office will gladly assist you in this process if you are unsure which type is the best match for the employee.

SIDA ID badge (RED TRIM AROUND EDGES) – individual has access privileges to the airport SIDA and does not require an escort

All applicants requesting a Westchester County Airport ID with unescorted access to the airport SIDA must submit to the following:

- Stipulated forms of identification and personal data
- An FBI fingerprint application for a Criminal Record History Check.
- A Security Threat Assessment
- Attendance at the airport SIDA training course.

AOA ID badge (GREEN TRIM AROUND EDGES) – Individual has unescorted access privileges to the Aeronautical Operations Area, including a FBO, tenant or small general aviation (GA) ramps. AOA badge holders are prohibited the access to SIDA area, unless under escort by a SIDA badge holder.

AOA ID badge holders are assigned one of the following endorsements, which further specify the areas in which they are allowed to be:

SENSITIVE SECURITY INFORMATION

- **FBO** – individual has unescorted access privileges to FBO/NetJets ramps but *requires an escort* to be on the airport SIDA.
- **CO** – individual has unescorted access privileges to the ramp of the tenant under which the ID has been issued, but *requires an escort* to be on the airport SIDA.
- **GA** – This card is issued to the small general aviation tenants (usually owners, renters, flight students or flying club members). Individuals with this type of the airport ID have a limited access to the AOA. The use of this identification card is limited to Landmark West and Million Air general aviation tiedown ramps. This card does not provide access, and it is not valid means of identification at any other part of the HPN AOA or SIDA.

Applicants requesting an AOA ID must submit to the following:

- Stipulated forms of identification and personal data (ALL APPLICANTS)
- An FBI fingerprint application for a Criminal Record History Check (APPLICABLE TO “FBO” ENDORSEMENT APPLICANTS ONLY)
- Completed 10-year employment history verification (APPLICABLE TO “CO” ENDORSEMENT APPLICANT ONLY)
 - a. If the employment history verification is missing or incomplete, the Airport ID office reserves the right to fingerprint applicant as a substitute for 10-year employment history
 - b. Authorized Signer will receive the courtesy call from this office for the confirmation of this procedure
- A Security Threat Assessment (ALL APPLICANTS)
- AOA security brief/training sheet (ALL APPLICANTS)

Tenants **MUST NOT** issue facility access cards or otherwise enable an individuals’ access to their ramps to any individuals with no airport ID badge or expired airport ID badge.

SENSITIVE SECURITY INFORMATION

Facility Access Policies

1. The company I represent operates the facility/hangar at the airport with direct access to the airfield (AOA)?

NO	If the answer is "NO" skip to the question #10	YES	If "YES", continue to the question #2
-----------	--	------------	---------------------------------------

2. Westchester County Airport transfers the responsibility of managing the access to the AOA as specified in 49 CFR TSR 1542 to its' tenants. You are required to answer these questions if your facility uses a proprietary access control system (the system that is not maintained and controlled by the Airport Security department).

How many total access points from the public area of the facility leading directly into the AOA (including vehicle and pedestrian gates outside the facility)?

3. How many total *internal* access points from the public area of the facility into the AOA (**do not** include external vehicle and pedestrian gates in this count)?

4. Are all the access points in the facility leading from the public into the AOA controlled by the access control system that is capable of preventing and detecting the unauthorized entry?

YES	If the answer is "YES" skip to question #7	NO	If the answer is "NO" go to the next question
------------	--	-----------	---

5. If not all the doors/gates with direct access to the AOA are operated by the access control system, how many of them are protected by the key/lock system.

6. Are all the keys issued for this/these locks accounted for?

YES	Go to the question #7	NO	If "NO" please contact Airport Security
------------	-----------------------	-----------	---

7. I am aware of the TSA and Westchester County Airport rule that no individual can be granted unescorted AOA access without going through the airport ID process and obtaining necessary security background checks through the Airport Security.

YES		NO	
------------	--	-----------	--

8. I understand that no individual with an expired airport ID can be granted access to the AOA and that facility access cards shall be deactivated immediately at all AOA access points upon the airport ID expiration date.

YES	Initial here please	NO	
------------	---------------------	-----------	--

9. I understand that any violation of these rules (#7 and #8), if observed by the TSA personnel inspecting the airfield, can lead to civil penalties in excess of \$11,000 and/or disciplinary actions by the Airport Security, including the temporary or permanent suspension or revocation of the airport ID.

YES		NO	
------------	--	-----------	--

10. My company has a system to track the expiration dates for airport badges that I and other Authorized Signers from my company are responsible for, and I disable the AOA access for all airport ID holders at my facility (if applicable) who fail to renew their airport ID before the expiration date.

YES		NO	
------------	--	-----------	--

SENSITIVE SECURITY INFORMATION

TEST:

1. The requirements for a person to become an Authorized Signatory are:
 - a) passing all required background checks
 - b) attend annual Authorized Signatory training
 - c) pass airport security training courses
 - d) all of these

2. The airport relies on _____ to help determine badge types each company employee needs in order to do their job.
 - a) authorized signatory
 - b) the police
 - c) FAA
 - d) TSA

3. Authorized signatories have the critical responsibility of complying with _____ within the airport's requested time frame.
 - a) TSA mandated badge audits
 - b) FAA Cert inspections
 - c) passing a security threat assessment
 - d) missing paperwork and incomplete ID forms

4. Airport ID badges must be immediately deactivated _____.
 - a) when an employee leaves the company and if a badge is lost or stolen
 - b) by TSA
 - c) as a test on a regular basis
 - d) when an employee goes on break

5. Common reasons for delays in applicants getting their badges that can be prevented are
 - a) keeping appointment times
 - b) passing a security threat assessment
 - c) missing paperwork and incomplete forms of ID
 - d) passing a criminal history record check

6. Authorized signatories should only send employees with _____ to the ID badging office
 - a) paperwork having TSA signatures
 - b) examined and confirmed required ID forms
 - c) paperwork examined by the FAA
 - d) company uniform

SENSITIVE SECURITY INFORMATION

<u>IMPORTANT PHONE NUMBERS</u>	
AIRPORT SECURITY DEPARTMENT:	
AIRPORT ID OFFICE: (914)-995-4009 HOURS: M-F 7AM-4PM SAT 8AM-4PM	
SARAH CESPEDES – AIRPORT SECURITY SUPERVISOR (914) 995 – 2592 (914) 490 – 0486 sac3@westchestergov.com	STEVEN FOURNIER – AIRPORT SECURITY SUPERVISOR (914) 995 – 2592 (914) 995-4009 snfa@westchestergov.com
AIRPORT OPERATIONS – 24/7 (914) 995 – 4850 For ID office hours and emergency notifications of lost badges that need to be deactivated ASAP	
STEPHEN FERGUSON – AIRPORT SECURITY COORDINATOR (914) 995 - 4855	LAURA GUERCIO – AIRPORT SECURITY MANAGER (914) 995 – 2748 (914) 467 – 0322 lega@westchestergov.com

I clearly understood all the duties and responsibilities of an Authorized Signer at Westchester County Airport as explained to me by the Airport Security Department staff during the training session summarized in this document. I was provided a reference copy of this document and I understand that this document is intended to be used only by Authorized Signers on file with Westchester County Airport, not to be copied or distributed.

TRAINEE (Authorized Signer)	TRAINER (Airport Security Representative)
PRINTED NAME	PRINTED NAME
SIGNATURE	SIGNATURE

Training conducted on (date): _____

CHRC date: _____ STA date: _____ SIDA course date: _____

For Airport Security Department use: Keep on file until retraining, but not less than 12 months from date of training

SENSITIVE SECURITY INFORMATION

WARNING: THIS RECORD CONTAINS SENSITIVE SECURITY INFORMATION THAT IS CONTROLLED UNDER 49 C.F.R. PARTS 15 AND 1520. NO PART OF THIS RECORD MAY BE DISCLOSED TO PERSONS WITHOUT A "NEED TO KNOW," AS DEFINED IN 49 C.F.R. PARTS 15 AND 1520, EXCEPT WITH THE WRITTEN PERMISSION OF THE ADMINISTRATOR OF THE TRANSPORTATION SECURITY ADMINISTRATION OR THE SECRETARY OF TRANSPORTATION. UNAUTHORIZED RELEASE MAY RESULT IN CIVIL PENALTIES OR OTHER ACTION. FOR U.S. GOVERNMENT AGENCIES, PUBLIC DISCLOSURE GOVERNED BY 5 U.S.C. 552 AND 49 C.F.R. PARTS 15 AND 1520.