METROPOLITAN WASHINGTON
AIRPORTS AUTHORITY

Airport Bulletins

Ronald Reagan
Washington National Airport

JUNE 2002
## TABLE OF CONTENTS

<table>
<thead>
<tr>
<th>No.</th>
<th>Document Type</th>
<th>Subject</th>
<th>Date</th>
<th>Pages</th>
</tr>
</thead>
<tbody>
<tr>
<td>01</td>
<td>Orders &amp; Instructions DCA 6-4-4A</td>
<td>Washington National Airport Identification Badge Requirements, dated July 10, 1991</td>
<td>20 Pages</td>
<td></td>
</tr>
<tr>
<td>03</td>
<td>Airport Advisory DCA 01/029</td>
<td>AOA Vehicle Gates, dated November 6, 2001</td>
<td>2 Pages</td>
<td></td>
</tr>
</tbody>
</table>
Orders & Instructions DCA 6-4-4A

Subject: Washington National Airport Identification Badge Requirements

Dated July 10, 1991

20 Pages
Metropolitan Washington Airports Authority
ORDERS & INSTRUCTIONS

SUBJECT: WASHINGTON NATIONAL AIRPORT IDENTIFICATION BADGE REQUIREMENTS

ISSUANCE DATE: 7/10/91

1.0 PURPOSE.

This Orders & Instructions (O&I) details the step-by-step procedures required in order to obtain a Washington National Airport (DCA) Identification badge (ID badge). This O&I is promulgated under the authority of Federal Aviation Regulation, Part 107 and Metropolitan Washington Airports Regulation (MWAR), Part 159.

2.0 DISTRIBUTION.

This O&I is distributed to Metropolitan Washington Airports Authority (the Authority) branch level and above, all airlines, tenants, concessionaires, and service companies conducting business at Washington National Airport.

3.0 CANCELLATION.

O&I DCA 6-4-4, Restricted Area and Air Operations Area (AOA) Photo ID Credentials, dated February 23, 1988.

4.0 REFERENCES.


c. Metropolitan Washington Airports Regulation, Part 159.


e. Washington National Airport Security Program, revised 12/90, and changes thereto.

Distribution: DCA-3/Airlines/Tenants/Concessionaires/Service Companies

OPI: MA-110

MWAA form 1236-1 (Oct. 1990)
5.0 ENCLOSURES.

a. Sample (Display) of DCA ID badges.

b. Request for Refund, MWAA Form 1129.

c. ID Badge/AOA Motor Vehicle Operator Permit Application, MWAA Form 4671A.


e. List of Washington National Airport AOA gates and doors equipped with card readers.


6.0 DEFINITIONS.

a. Air Operations Area (AOA).

That portion of Washington National Airport used or intended to be used for landing, takeoff or surface maneuvering of aircraft.

b. Airport Access Control System (AACS).

A computer-based access control system designed for and installed at Washington National Airport.

c. Contractor.

A contractor, as used throughout this O&I, is an individual or individuals that represent a service company with a contractual agreement to do work at Washington National Airport.

d. Employer.

An employer, as used throughout this O&I, is the individual who is responsible for all of his/her organization's activities at Washington National Airport.

e. Personal Identification Number (PIN).

A four-digit number chosen by an individual for use with the DCA ID badge.

f. Restricted Area.

That portion of Washington National Airport that is not intended for public use or access. The restricted areas include the AOA. They are areas designated by the Airport Manager as restricted areas and clearly identified with signs designating them as "RESTRICTED AREAS."
7.0 THE DCA ID BADGE.

Each new DCA ID badge will be issued to a specific individual and is not transfeerrable to another individual. Each new DCA ID badge holder will also have an individual PIN assigned. Use by a person other than the person to whom the DCA ID badge and/or PIN was issued will result in the confiscation of the DCA ID badge by airport security personnel. All persons who are on the AOA and/or in a restricted area at Washington National Airport shall overtly display on an outer garment, above the waist but below the neck, a DCA ID badge.

a. TYPES OF DCA ID BADGES.

There are two types of DCA ID badges, REGULAR ID BADGE and TEMPORARY ID BADGE. Samples (displays) of each type of DCA ID badge are shown in Enclosure A, figures A, B and C.

(1) REGULAR - DCA ID badges will only be valid for a 12-month period, expiring on the last day of the individual’s birth month. The ONLY EXCEPTION is a contractor DCA ID badge with an expiration date of less than 1 year which will expire on the job completion date.

The DCA ID badge is for individuals who are assigned to or have continuing, frequent presence at DCA, such as DCA tenants, concessionaires, contractors, off-airport vendors and other service firms or agencies, and who are authorized unescorted access to the DCA AOA and/or restricted areas.

(2) TEMPORARY - DCA ID badge is only issued to an individual who has a current REGULAR DCA ID badge. Occasionally an individual will forget his/her DCA ID badge and is sure of the location of the DCA ID badge. Under the above stated conditions, a TEMPORARY DCA ID badge may be issued for only 1 day (24 hours), and the individual’s REGULAR DCA ID badge will be deactivated.

The TEMPORARY DCA ID badge must be returned to the Airport ID and Driver Permit Office before the REGULAR DCA ID badge will be reactivated. (DCA ID badges may be returned to the Operations Office after normal business hours.)

b. DCA ID BADGE COLORS.

There are four different DCA ID badge colors.

The color of the DCA ID badges, REGULAR and TEMPORARY, is intended to provide an immediate visual cue as to the access authorized the individual overtly displaying his/her DCA ID badge.
(1) **RED** - Restricted Area Access.

(2) **YELLOW** - Restricted Area Access, excluding all AOA areas.

(3) **BLUE** - Limited Area Access. General Aviation ramp and University of DC area.

(4) **WHITE** - No access to any restricted area.

c. **DCA ID BADGE FEES.**

The following schedule of fees applies to the DCA ID badge indicated. Fees are payable to MWAA at the Authority Agent Cashier's Office (Main Terminal, Room 220) in advance of the DCA ID badge being issued.

(1) **REGULAR DCA ID BADGE (EMPLOYEES)**

<table>
<thead>
<tr>
<th>Description</th>
<th>Fee</th>
</tr>
</thead>
<tbody>
<tr>
<td>Initial issue</td>
<td>$10.00</td>
</tr>
<tr>
<td>First reissue*</td>
<td>$50.00</td>
</tr>
<tr>
<td>Second reissue*</td>
<td>$100.00</td>
</tr>
<tr>
<td>Third reissue*</td>
<td>$200.00</td>
</tr>
<tr>
<td>Annual (on-time) Renewal**</td>
<td>$5.00</td>
</tr>
<tr>
<td>Annual (late) Renewal**</td>
<td>$10.00</td>
</tr>
</tbody>
</table>

* Reissue is defined as replacement of a lost, stolen or damaged DCA ID badge. (See paragraph 8f.)

** See paragraph 8e.

A third reissue DCA ID badge will not be issued without the written authorization of the Airport Manager, Washington National Airport.

Replacement of an inoperable DCA ID badge will be free of charge.

(2) **REGULAR DCA ID BADGE (CONTRACTORS ONLY)**

<table>
<thead>
<tr>
<th>Description</th>
<th>Fee</th>
</tr>
</thead>
<tbody>
<tr>
<td>Initial issue</td>
<td>$50.00</td>
</tr>
<tr>
<td>Renewal (on-time) and Replacement</td>
<td>$5.00</td>
</tr>
<tr>
<td>Renewal (late)</td>
<td>No Reissue</td>
</tr>
</tbody>
</table>
First, second and/or third reissue of a lost, stolen or damaged DCA ID badge for a contractor will be in accordance with the fee schedule in paragraph 7c(1) above. Replacement of an inoperable DCA ID badge for a contractor will be free of charge.

Contractors' DCA ID badges that have expired and need to be renewed (to complete the job for which the DCA ID badges were issued) may be renewed at a fee of $5.00. (See paragraph 8e(1) for renewal procedures.)

(3) **TEMPORARY DCA ID BADGE.**

NO CHARGE. The total number of TEMPORARY DCA ID badges that will be issued to any individual in any 1-year period is two. The 1-year period begins on the date the REGULAR DCA ID badge is issued.

d. **DCA ID BADGE HOLDER REFUND.**

(1) When a REGULAR DCA ID badge holder (including a contractor), who has properly reported the loss of his/her DCA ID badge and has been issued a replacement DCA ID badge, recovers his/her lost DCA ID badge, the individual will be entitled to a refund for returning the lost badge in accordance with the following schedule of fees:

<table>
<thead>
<tr>
<th>ID BADGE</th>
<th>REFUND</th>
</tr>
</thead>
<tbody>
<tr>
<td>First replacement</td>
<td>$30.00</td>
</tr>
<tr>
<td>Second replacement</td>
<td>$80.00</td>
</tr>
<tr>
<td>Third replacement</td>
<td>$180.00</td>
</tr>
</tbody>
</table>

(2) When a contractor completes a job at Washington National Airport, all DCA ID badges must be returned to the Airport ID and Driver Permit Office within 10 days of the expiration date of the DCA ID badge. A contractor is entitled a refund of $40.00 for each DCA ID badge returned. No refund will be given for a DCA ID badge that is not returned within 10 days after the DCA ID badge expires and future issuance of DCA ID badges may be denied.

When a DCA ID badge holder refund is appropriate, the Airport ID and Driver Permit Office shall assist the individual in filling out a Request For Refund (see Enclosure B).
e. **DCA ID BADGES REMAIN MWAA PROPERTY.**

The DCA ID badge is and remains the property of the Authority and shall be surrendered upon the demand of the Authority or its officials. Any attempt by a DCA ID badge holder to help, assist, aid or abet anyone to bypass the Washington National Airport AACS will not only compromise airport security, but will also subject the card holder to revocation of his/her possession of a DCA ID badge and legal prosecution under references in paragraph 4 above, and any applicable Federal or State law.

f. **MULTIPLE EMPLOYERS.**

In cases where an individual is employed by more than one employer at Washington National Airport, the employee must complete an ID Badge/AOA Motor Vehicle Operator Permit Application (see Enclosure C) for each employer. All employers are responsible for ensuring that each employee who requires a DCA ID badge has completed Section I of the application form and that the proper background check has been performed. The fee for the DCA ID badge will only be required with the first application, considered to be the primary employer. Any changes in employment status must be reported immediately as outlined in paragraphs 8c and 9a and 9b below, as appropriate.

g. **PAYMENT OF DCA ID BADGE FEES.**

The payment of fees shall be accepted only by the Authority Agent Cashier’s Office by one of the following methods:

1. Cash

2. Check (made payable to MWAA).

3. Voucher (as approved by the Airport Manager).

The Authority Agent Cashier’s Office will not accept payment from any applicant until the application form has been approved by the Airport ID and Driver Permit Office. If checks received are returned to the Authority for insufficient funds, the DCA ID badge will immediately be removed from the AACS. Reissue will be at the highest fee rate cited in paragraph 7c above, subject to the Airport Manager’s approval. A $10.00 charge will be assessed for all returned checks.
h. INITIAL AND RENEWAL ISSUE FEE WAIVER.

The payment of the fee for the initial and renewal issue of the DCA ID badge is waived for all employees of the Authority and Federal Government entities. The fee for all lost or stolen DCA ID badges is not waived and will be in accordance with the fee schedule set forth in paragraph 7c(1) above.

8.0 DCA ID BADGE ISSUANCE PROCEDURES.

The procedures detailed below are arranged in step-by-step order and must be followed for an individual to be issued a DCA ID badge. The procedures to make a change to a DCA ID badge already in the possession of an individual are also detailed in this section. These procedures presume that the employer has on file a current Designated Certification Official letter (see Enclosure D).

The Airport ID and Driver Permit Office is located in the Main Terminal, Room 18. The hours of operation are Monday through Friday, 7 a.m. - 12 p.m. and 1 p.m. - 3 p.m., excluding holidays. All forms may be obtained in this office.

All non-English speaking/reading applicants must be accompanied by an English speaking/reading translator.

ALL APPLICATIONS MUST BE TYPED OR PRINTED LEGIBLY.

a. PROCEDURES.

(1) The employer must provide the applicant for whom a DCA ID badge is required an ID Badge/AOA Motor Vehicle Operator Permit Application (See Enclosure C).

(2) The applicant must complete and sign Section I of the form.

(3) The applicant must read, understand, agree to comply with, sign and date the Security Responsibility Agreement on the reverse side of the application form.

(4) The employer must complete Section II of the application form. The employer must state whether an AOA key, AOA access, an AOA Motor Vehicle Operator Permit and/or AOA doors/gates are required.
(a) If AOA access is requested, the employer must indicate the specific access level required from the list of doors and gates provided in Enclosure E. The access level shall be limited to only those gates and doors necessary for an employee to perform his/her job duties.

(b) If an AOA Motor Vehicle Operator Permit is requested, the applicant must be prepared to be tested on the DCA AOA driving rules and regulations (Reference O&I DCA 3-2-1G). NO DCA ID badge will activate an AOA vehicle gate until the applicant successfully passes the driver exam.

(5) The employer must certify that a 5-year background investigation (employment, educational and/or personal reference) of the applicant has been performed and that this check appears on the reverse side of the application by completing Section V. The employer must account for all time. If any gaps are apparent, the application will be rejected.

(6) Part II of the application form must be signed by one of the company's designated certification officials. Signature comparisons will be made with the letter on file in the Airport ID and Driver Permit Office.

(7) The employer, by signing the application form, acknowledges the responsibility to ensure that the applicant has:

(a) Successfully demonstrated his/her ability to operate motor vehicles on the AOA.

(b) Been properly indoctrinated in airport security and understands the contents of this O&I.

(8) The applicant must then carry his/her application form to the Airport ID and Driver Permit Office.

(9) The Airport ID and Driver Permit Office will review the application. When the application form is approved, the Airport ID and Driver Permit Office will determine the fee to be paid and initial the first part of Section III on the application form.
(10) The applicant must carry the approved application form to the Authority Agent Cashier's Office located in the Main Terminal, Room 220, where the fee will be collected. The Agent Cashier will not accept payment unless the application is first approved by the Airport ID and Driver Permit Office. The Agent Cashier will check the form of payment received and indicate the receipt number assigned for a cash/check transaction. This completes Section III of the application form.

(11) The applicant must carry the application form back to the Airport ID and Driver Permit Office where a DCA ID badge will be issued. The applicant will choose his/her PIN and the Airport ID and Driver Permit Office will record the PIN in the AACS.

(12) The Airport ID and Driver Permit Office will test the new DCA ID badge and PIN with the applicant present to ensure that the new DCA ID badge holder understands how the DCA ID badge and PIN are to be used.

(13) If an AOA Motor Vehicle Operator Permit is required, an exam will be given by the Airport ID and Driver Permit Office. Once the applicant successfully passes the exam, the DCA ID badge will be issued with the word DRIVER on the right side of the applicant's picture, authorizing the applicant to drive on the AOA. (Reference O&T DCA 3-2-1G.)

NO DCA ID BADGE WILL BE ISSUED UNLESS ALL OF THE ABOVE STEPS ARE FOLLOWED.

b. ADDITIONAL CONTRACTOR REQUIREMENTS.

DCA ID badges will only be issued to contractors who have been issued an Airport work permit to perform work for the Authority or Airport tenants. DCA ID badges will be for the duration of the specified project/contract or 12 months, whichever is the shorter period.

Applications for DCA ID badges must be submitted to and reviewed by the Parsons Management Consultants (PMC) Office Manager or the Authority Engineering Project Manager prior to processing by the Airport ID and Driver Permit Office. The Airport ID and Driver Permit Office will not accept applications which do not have a signed original PMC or Authority Engineering Division cover letter detailing the project and a Request for Contractor Credential form (see Enclosure F).
c. **UPDATING DCA ID BADGE INFORMATION PROCEDURES.**

If the data submitted on the application form to obtain a REGULAR DCA ID badge changes, the employer shall notify the Airport ID and Driver Permit Office in writing by submitting a revised ID Badge/AOA Motor Vehicle Operator Permit Application (See Enclosure C). No fee will be charged for this service unless a new DCA ID badge is necessary.

d. **TEMPORARY DCA ID BADGE (FORGOTTEN BADGE) PROCEDURES.**

If a REGULAR DCA ID badge holder has forgotten his/her REGULAR DCA ID badge (NOT LOST, STOLEN or DAMAGED), he/she may be issued a TEMPORARY DCA ID badge which is good for 1 day (24 hours). During normal working hours, an employee may proceed to the Airport ID and Driver Permit Office. During non-normal working hours, proceed to the Airport Operations Office, Main Terminal, Room 26C. Upon presentation of authorization by the company's designated certification official or supervisor and a picture ID card, a TEMPORARY DCA ID badge may be issued. The AACS will automatically deactivate the employee's REGULAR DCA ID badge until the TEMPORARY DCA ID badge is returned to the Airport ID and Driver Permit Office.

This privilege will be granted only two times during any 1-year period. This 1-year period begins the day the REGULAR DCA ID badge is issued. After the second time, the DCA ID badge holder will be required to use his/her REGULAR DCA ID badge or carry out the provisions of paragraph 8f below.

e. **DCA ID BADGE RENEWAL/REPLACEMENT PROCEDURES.**

1. **RENEWAL.**

At least 10 days prior to the date that a REGULAR DCA ID badge expires, the DCA ID badge holder must go to the Airport ID and Driver Permit Office to renew his/her DCA ID badge. The Airport ID and Driver Permit Office will pull the individual's original application form(s) and review the form(s) with the individual to ensure that all information is current and correct. If any information has changed, a new application form is required. With the return of the expiring DCA ID badge, a new DCA ID badge with a revised expiration date will then be issued at a cost of $5.00. (See paragraph 7c(1) and (2).)
If a DCA ID badge holder does not renew his/her DCA ID badge prior to the expiration date, a renewal DCA ID badge will not be issued without written authorization from the employer stating that the individual is a current employee. If any information has changed, a new application form is required. A DCA ID badge will be issued at a cost of $10.00. (See paragraph 7c(1).)

A renewal DCA ID badge will not be issued to a contractor whose DCA ID badge has expired. (See paragraph 7c(2).)

(2) REPLACEMENT.

If the DCA ID badge becomes inoperable, for any reason, the DCA ID badge holder shall return that DCA ID badge to the Airport ID and Driver Permit Office, and a replacement DCA ID badge will be issued at no cost. The Airport ID and Driver Permit Office will pull the original application form and review the form with the individual to ensure that all information is still correct. If any information has changed, a new application form is required.

f. DCA ID BADGE REISSUE PROCEDURES.

The DCA ID badge holder must IMMEDIATELY notify the Airport ID and Driver Permit Office (703-685-8052) or the Airport Operations Office (703-685-8050) if his/her DCA ID badge is lost, unaccounted for, or stolen. A replacement DCA ID badge will be issued if the applicant follows the appropriate steps outlined in paragraph 8a above and after the appropriate fee as outlined in paragraph 7c above, has been paid.

9.0 TERMINATION OF AN EMPLOYEE, CONTRACTOR OR VENDOR DCA ID BADGE.

a. Employers shall IMMEDIATELY notify the Airport ID and Driver Permit Office or the Airport Operations Office whenever an employee, contractor or vendor having a valid DCA ID badge is terminated. The Airport ID and Driver Permit Office or the Airport Operations Office will IMMEDIATELY remove that individual’s AOA access from the AACS. The employer must provide written confirmation of this information within 24 hours to the Airport ID and Driver Permit Office. The reason for termination shall be included in the written statement.

b. The employer shall collect the employee’s DCA ID badge and any AOA door key(s) issued and return them to the Airport ID and Driver Permit Office within 5 working days.
10.0 **UNAUTHORIZED USE OF A DCA ID BADGE.**

a. A DCA ID badge used by a person other than the individual to whom it was issued will be confiscated by any Airport security personnel observing the unauthorized use. The DCA ID badge will not be returned to the individual to whom it was issued until authorized by the Manager, Airport Operations Division.

b. Any individual who willfully allows any other person to use his/her DCA ID badge and/or PIN will have such DCA ID badge confiscated, will have his/her access immediately removed from the AACS computer and will be referred to his/her supervisor for disciplinary action. If the employer requests reissue, the reissue will follow the procedures outlined in paragraph 8a above, at the highest fee listed in paragraph 7c above; however, Airport Management reserves the right to refuse reissue.

c. Any person witnessing the unauthorized use of a DCA ID badge shall **IMMEDIATELY** report this to the Airport Operations Office.

11.0 **ESCORT PROCEDURES.**

Individuals who are REGULAR DCA ID badge holders may escort temporary visitors who are not authorized access to the restricted and/or AOA areas of the airport, provided the DCA ID badge holder is authorized such access. It is the responsibility of the DCA ID badge holder to ensure the person(s) being escorted remains within 10 feet in line of sight of him/her at all times. If the person is challenged by an airport employee or security personnel, the person shall reply, "I am being escorted by ___________ (escort's name)" and point to the DCA ID badge holder acting as escort. If at any time the individual does not follow the ID badge holder's directions, the DCA ID badge holder shall contact the Airport Police and Airport Operations Office immediately and have the violator(s) removed from the restricted and/or AOA area.

[Signature]
Augustus A. Melton, Jr.
Airport Manager
Washington National Airport

6 Enclosures
Figure - A

GULAR DCA ID BADGE

Drivers Permit Symbol (Non-drivers ID Badge will be blank in this area)

Badge Holder's Name

Company

Expiration Date

Month

Year

Badge Number

Figure - B

Back of both REGULAR and TEMPORARY ID BADGE

Figure - C

A TEMPORARY DCA ID BADGE

Temporary Symbol

Expiration Date of Temporary
**REQUEST FOR REFUND**

**PART A. TO BE COMPLETED BY APPLICANT**

Application is hereby made for refund of fees or property deposited with MWAA. Refund should be sent to (Please Print):

<table>
<thead>
<tr>
<th>STREET ADDRESS</th>
<th>CITY, STATE, ZIP</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>IN:</th>
<th>CONTACT PERSON</th>
<th>DAYTIME PHONE</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

**PART B. TO BE COMPLETED BY APPLICANT (COMPLETE SECTIONS 1 AND 2)**

Description of fees or property refund is requested for:

- ☐ Return of Credentials
- ☐ Unclaimed Property
- ☐ Overpayment
- ☐ Other (Describe)

Calculation of amount due:

<table>
<thead>
<tr>
<th>AMOUNT CLAIMED</th>
<th>AMOUNT DUE</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
</tr>
</tbody>
</table>

- Credentials Returned @ $ Per Credential =
- Other (Describe)
- Total

I certify that the information above is correct and that payment has not already been received.

SIGNATURE OF REQUESTOR

DATE

**PART C. TO BE COMPLETED BY MWAA REPRESENTATIVE**

The above described property (has been):

- ☐ Returned
- ☐ Deposited With
- ☐ Is Due to the Above Named Vendor

The amount due is $_____

MWAA representative describe any difference between the amount in Part B and Part C:

**PART D. TO BE COMPLETED BY ACCOUNTING**

CODING

DATE PROCESSED

INITIALS
ID BADGE/AOA MOTOR VEHICLE OPERATOR PERMIT APPLICATION

SECTION I — APPLICANT

Print legibly or type.

S Name, First, MD

License No. STATE EXPIRATION DATE DATE OF BIRTH SOCIAL SECURITY NO.

WEIGHT RACE COLOR OF HAIR COLOR OF EYES

FOR TITLE HIRE DATE WITH PRESENT EMPLOYER

I understand that any unanswered questions and any false or misleading information on this application may be cause this application to be disapproved or for any permit or ID badge issued as a result to be revoked.

I have read, fully understand, and agree to abide by the Security Responsibility Agreement on the reverse side of this application.

I understand that failure on my part to follow any security procedures may result in the revocation of my ID badge, AOA legal actions, and that I may be banned from the restricted areas of Washington National Airport.

ANY'S SIGNATURE

SECTION II — EMPLOYER — DESIGNATED CERTIFICATION OFFICIAL

TELEPHONE NO.

AGA DOOR KEY REQUIRED? Yes No

ACCESS REQUIRED AOA OPERATOR PERMIT REQUIRED AOA ACCESS AND AOA OPERATOR PERMIT ARE MANDATORY FOR ANY APPLICANT REQUIRING VEHICLE GATE.

AOA GATE/DOORS REQUIRED:

YES NO

5 OF ID BADGE (Check applicable box): New Applicant Lost Temporary

Damaged Expiration Date

Designated Certification Official's Name and Title (Print or Type)

I certify that upon termination or loss of the ID badge or AOA key, it is my company's or agency's responsibility to notify Operations Division immediately, but not more than 24 hours, after the termination or loss at (703) 685-8050.

I certify that verification of the above applicant's previous 5 years of employment or educational history or any personal references has been conducted and appears on the reverse side of this application and is accurate to the best of my knowledge.

I certify that this applicant has successfully demonstrated his/her ability to operate motor vehicle(s) required to perform his/her job duties.

My company or agency will reimburse the Metropolitan Washington Airports Authority for any FAA fines levied against Washington National Airport which are caused by the failure of one or our employees to adhere to the Washington National Airport Security Program.

Signature

DATE

SECTION III — OPERATIONS DIVISION/AGENT CASHIER'S USE ONLY

PAYMENT: initial$ Form of Payment: Voucher Cash/Check Receipt No.

SECTION IV — DCA OPERATIONS DIVISION USE ONLY

BADGE NO.

ISSUE DATE

ACCESS GROUP NO.
IV. 5-YEAR EMPLOYMENT, EDUCATION AND PERSONAL HISTORY CHECKS

<table>
<thead>
<tr>
<th>APPLICANT</th>
<th>COMPANY/ORGANIZATION</th>
<th>PERSON CONTACTED/TITLE</th>
<th>TELEPHONE NO.</th>
<th>PERSON CONDUCTING VERIFICATIONS</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

1. A full account of the applicant's 5-year employment, educational or personal history must be provided.

2. All time must be accounted for. This application will be disapproved if there are any gaps.

---

**Metropolitan Washington Airports Authority**

**SECURITY RESPONSIBILITY AGREEMENT**

I will not allow anyone else to use this ID badge or AOA key.

I will properly display my ID badge at all times, and wear the ID badge on my outermost garment when in a restricted area.

I will challenge any individual who fails to display an ID badge.

I understand that ID badges with a yellow background grant sterile area access only, not AOA access.

I will ensure proper closing and locking of any AOA door or gate used.

I will not allow any individual to follow me or my vehicle through any AOA door or gate.

I will report the theft or loss of my ID badge or AOA key immediately to the Airport Operations Division.

I will report immediately any security violation I witness to the Airport Operations Division or the Airport Police.

I have read and understand that failure to comply with any or all of the above security procedures may result in the revocation of my ID badge or AOA key and possible banning from the restricted area of the Airport.

APPLICANT'S SIGNATURE

DATE
Enclosure D

WASHINGTON NATIONAL AIRPORT

DESIGNATED CERTIFICATION OFFICIAL LETTER

(SAMPLE - DO NOT USE AS ORIGINAL)

Manager, Operations Division, MA-110
Washington National Airport
Washington, DC 20001

Dear Sir:

The purpose of this letter is to advise you of [Company Name] activities at Washington National Airport and request authorization to apply for security identification badges.

[Company Name] is engaged in (a brief description of your activities at Washington National Airport to include locations on the Airport where proposed activities will occur, and the reason why your employees will require access to the secure area of the Airport).

To fulfill the requirements of the Washington National Airport Security Program and Orders and Instructions (O&I) DCA 6-4-4, the following individual(s) are designated as certification official(s) (must be a company officer or their local management representative) and their sample signature(s) appear below.

EXAMPLE:

John T. Doe Vice President X__________
Jane C. Smith Secretary X__________
Tom A. Jones Station Manager X__________

The above-named individuals are familiar with the Airport Security Program and will ensure [COMPANY NAME] employees who are issued Washington National Airport ID badges comply with the Program. [COMPANY NAME] will ensure a strict accounting of all DCA ID Badges is maintained, to include prompt reporting of any lost badges and return of DCA ID badges upon termination or transfer of any employee.

I certify that any Federal Aviation Regulation fine levied against the Airport as a result of any [COMPANY NAME] employee's failure to adhere to the Washington National Airport Security Program will be paid by the [COMPANY NAME].

Sincerely,

Signature

[COMPANY OFFICER OR LOCAL MANAGER]
### Washington National Airport AOA Access Doors with Card Readers

<table>
<thead>
<tr>
<th>Reader No.</th>
<th>NAME</th>
<th>LOCATION</th>
<th>REMARKS</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Gate V</td>
<td>North end of airport</td>
<td>In</td>
</tr>
<tr>
<td>2</td>
<td>Gate V</td>
<td>North end of airport</td>
<td>Out</td>
</tr>
<tr>
<td>9</td>
<td>Baggage Rm</td>
<td>Hangar 11</td>
<td>In</td>
</tr>
<tr>
<td>10</td>
<td>Baggage Rm</td>
<td>Hangar 11</td>
<td>Out</td>
</tr>
<tr>
<td>11</td>
<td>Elevator</td>
<td>Hangar 11</td>
<td>In</td>
</tr>
<tr>
<td>12</td>
<td>Elevator</td>
<td>Hangar 11</td>
<td>Out</td>
</tr>
<tr>
<td>17</td>
<td>N. Door</td>
<td>Hangar 11</td>
<td>In</td>
</tr>
<tr>
<td>18</td>
<td>N. Door</td>
<td>Hangar 11</td>
<td>Out</td>
</tr>
<tr>
<td>19</td>
<td>Stair 2</td>
<td>Hangar 11 (Anton's)</td>
<td>In</td>
</tr>
<tr>
<td>20</td>
<td>Stair 2</td>
<td>Hangar 11 (Anton's)</td>
<td>Out</td>
</tr>
<tr>
<td>21</td>
<td>S. Door</td>
<td>Hangar 11</td>
<td>In</td>
</tr>
<tr>
<td>22</td>
<td>S. Door</td>
<td>Hangar 11</td>
<td>Out</td>
</tr>
<tr>
<td>25</td>
<td>Stair 4</td>
<td>Hangar 11 (Cargo Elev)</td>
<td>In</td>
</tr>
<tr>
<td>26</td>
<td>Stair 4</td>
<td>Hangar 11 (Cargo Elev)</td>
<td>Out</td>
</tr>
<tr>
<td>27</td>
<td>Stair 3</td>
<td>Hangar 11 (Jetway H-9)</td>
<td>In</td>
</tr>
<tr>
<td>28</td>
<td>Stair 3</td>
<td>Hangar 11 (Jetway H-9)</td>
<td>Out</td>
</tr>
<tr>
<td>29</td>
<td>Stair 1</td>
<td>Hangar 11 (USAir Club)</td>
<td>In</td>
</tr>
<tr>
<td>30</td>
<td>Stair 1</td>
<td>Hangar 11 (USAir Club)</td>
<td>Out</td>
</tr>
<tr>
<td>41</td>
<td>N. Tunnel</td>
<td>Main Terminal</td>
<td>In</td>
</tr>
<tr>
<td>42</td>
<td>N. Tunnel</td>
<td>Main Terminal</td>
<td>Out</td>
</tr>
<tr>
<td>43</td>
<td>Jetway 21</td>
<td>Main Terminal</td>
<td>In</td>
</tr>
<tr>
<td>44</td>
<td>Jetway 21</td>
<td>Main Terminal</td>
<td>Out</td>
</tr>
<tr>
<td>45</td>
<td>Tower</td>
<td>MT - 3rd Floor</td>
<td>In</td>
</tr>
<tr>
<td>46</td>
<td>Tower</td>
<td>MT - 3rd Floor</td>
<td>Out</td>
</tr>
<tr>
<td>49</td>
<td>Jetway 20</td>
<td>Main Terminal</td>
<td>In</td>
</tr>
<tr>
<td>50</td>
<td>Jetway 20</td>
<td>Main Terminal</td>
<td>Out</td>
</tr>
<tr>
<td>51</td>
<td>S. Tunnel</td>
<td>Main Terminal</td>
<td>In</td>
</tr>
<tr>
<td>52</td>
<td>S. Tunnel</td>
<td>Main Terminal</td>
<td>Out</td>
</tr>
<tr>
<td>53</td>
<td>Ops Door</td>
<td>Airport Operations</td>
<td>In</td>
</tr>
<tr>
<td>54</td>
<td>Ops Door</td>
<td>Airport Operations</td>
<td>Out</td>
</tr>
<tr>
<td>55</td>
<td>Test 1</td>
<td>Airport Operations</td>
<td>Ops Office</td>
</tr>
<tr>
<td>Reader No.</td>
<td>NAME</td>
<td>LOCATION</td>
<td>REMARKS</td>
</tr>
<tr>
<td>-----------</td>
<td>--------------</td>
<td>-------------------------</td>
<td>---------</td>
</tr>
<tr>
<td>56</td>
<td>Test 2</td>
<td>ID Office</td>
<td>ID Office</td>
</tr>
<tr>
<td>57</td>
<td>West Doors</td>
<td>AA/CO Terminal</td>
<td>In</td>
</tr>
<tr>
<td>58</td>
<td>West Doors</td>
<td>AA/CO Terminal</td>
<td>Out</td>
</tr>
<tr>
<td>59</td>
<td>Center Doors</td>
<td>AA/CO Terminal</td>
<td>In</td>
</tr>
<tr>
<td>60</td>
<td>Center Doors</td>
<td>AA/CO Terminal</td>
<td>Out</td>
</tr>
<tr>
<td>61</td>
<td>East Doors</td>
<td>AA/CO Terminal</td>
<td>In</td>
</tr>
<tr>
<td>62</td>
<td>East Doors</td>
<td>AA/CO Terminal</td>
<td>Out</td>
</tr>
<tr>
<td>63</td>
<td>Baggage Door</td>
<td>AA/CO Terminal</td>
<td>In</td>
</tr>
<tr>
<td>64</td>
<td>Baggage Door</td>
<td>AA/CO Terminal</td>
<td>Out</td>
</tr>
<tr>
<td>65</td>
<td>Gate N</td>
<td>Loading Dock</td>
<td>In</td>
</tr>
<tr>
<td>66</td>
<td>Gate N</td>
<td>Loading Dock</td>
<td>Out</td>
</tr>
<tr>
<td>67</td>
<td>PED M</td>
<td>Loading Dock</td>
<td>In</td>
</tr>
<tr>
<td>68</td>
<td>PED M</td>
<td>Loading Dock</td>
<td>Out</td>
</tr>
<tr>
<td>69</td>
<td>NW Baggage</td>
<td>Northwest Terminal</td>
<td>In</td>
</tr>
<tr>
<td>70</td>
<td>NW Baggage</td>
<td>Northwest Terminal</td>
<td>Out</td>
</tr>
<tr>
<td>73</td>
<td>N. Gate</td>
<td>Northwest Terminal</td>
<td>In</td>
</tr>
<tr>
<td>74</td>
<td>N. Gate</td>
<td>Northwest Terminal</td>
<td>Out</td>
</tr>
<tr>
<td>75</td>
<td>S. Gate</td>
<td>Northwest Terminal</td>
<td>In</td>
</tr>
<tr>
<td>76</td>
<td>S. Gate</td>
<td>Northwest Terminal</td>
<td>Out</td>
</tr>
<tr>
<td>81</td>
<td>S. Fire Door</td>
<td>Northwest Terminal</td>
<td>In</td>
</tr>
<tr>
<td>82</td>
<td>S. Fire Door</td>
<td>Northwest Terminal</td>
<td>Out</td>
</tr>
<tr>
<td>83</td>
<td>S. Office Door</td>
<td>Northwest Terminal</td>
<td>In</td>
</tr>
<tr>
<td>84</td>
<td>S. Office Door</td>
<td>Northwest Terminal</td>
<td>Out</td>
</tr>
<tr>
<td>85</td>
<td>N. Office Door</td>
<td>Northwest Terminal</td>
<td>In</td>
</tr>
<tr>
<td>86</td>
<td>N. Office Door</td>
<td>Northwest Terminal</td>
<td>Out</td>
</tr>
<tr>
<td>87</td>
<td>N. Fire Door</td>
<td>Northwest Terminal</td>
<td>In</td>
</tr>
<tr>
<td>88</td>
<td>N. Fire Door</td>
<td>Northwest Terminal</td>
<td>Out</td>
</tr>
<tr>
<td>89</td>
<td>Gate K</td>
<td>General Aviation</td>
<td>In</td>
</tr>
<tr>
<td>90</td>
<td>Gate K</td>
<td>General Aviation</td>
<td>Out</td>
</tr>
<tr>
<td>97</td>
<td>Gate F</td>
<td>Air Cargo Bldg</td>
<td>In</td>
</tr>
<tr>
<td>98</td>
<td>Gate F</td>
<td>Air Cargo Bldg</td>
<td>Out</td>
</tr>
<tr>
<td>99</td>
<td>Cargo 1</td>
<td>Tuggate</td>
<td>In</td>
</tr>
<tr>
<td>100</td>
<td>Cargo 1</td>
<td>Tuggate</td>
<td>Out</td>
</tr>
<tr>
<td>Reader No.</td>
<td>NAME</td>
<td>LOCATION</td>
<td>REMARKS</td>
</tr>
<tr>
<td>-----------</td>
<td>--------</td>
<td>--------------------</td>
<td>---------</td>
</tr>
<tr>
<td>101</td>
<td>Cargo 2</td>
<td>Tuggate</td>
<td>In</td>
</tr>
<tr>
<td>102</td>
<td>Cargo 2</td>
<td>Tuggate</td>
<td>Out</td>
</tr>
<tr>
<td>105</td>
<td>Gate B</td>
<td>Air Mail Facility</td>
<td>In</td>
</tr>
<tr>
<td>106</td>
<td>Gate B</td>
<td>Air Mail Facility</td>
<td>Out</td>
</tr>
<tr>
<td>113</td>
<td>Gate A</td>
<td>South End of Airport</td>
<td>In</td>
</tr>
<tr>
<td>114</td>
<td>Gate A</td>
<td>South End of Airport</td>
<td>Out</td>
</tr>
</tbody>
</table>
Airport Bulletin DCA 9/47

Subject: Expansion of Fingerprint Requirement of New Applicants Having Unescorted Airport Access, Security Screeners, and Their First Line Supervisors

Dated December 22, 2000

4 Pages
1. PURPOSE

This Airport Bulletin implements new procedures to obtain an ID badge at Ronald Reagan Washington National Airport to meet the requirements of recent Congressional legislation.

2. DISTRIBUTION

This Bulletin is distributed to all Metropolitan Washington Airports Authority branches and above, air carriers, tenants, government, concessionaires, and contractors at DCA.

3. GENERAL

On November 22, 2000, the President of the United States signed the Airport Security Improvement Act of 2000 into law (Public Law # 106-528). This Act directly impacts current requirements and procedures for passenger screeners, screener supervisors, and all positions requiring unescorted access to the Security Identification Display Area (SIDA), by amending Title 49 of the United States Code, Section 44936 Employment Investigations and Restrictions. The new law affects the FAA’s employment investigations rule Title 14 Code of Federal Regulations (CFR), Section 107.31 and 108.33. The effective start date of the Airport Security Improvement Act of 2000 shall be December 23, 2000, at 12:01 A.M.

4. PROCEDURES

Effective December 23, 2000, FBI Criminal History Record Checks, using fingerprinting, are required for all new airport employees who are seeking unescorted access to the SIDA.

All new non-airline tenant (FAR Part 107) applicants requesting access to the SIDA must be fingerprinted by DCA Pass & ID Office personnel. The fee of $29 for each employee may be paid by cash, credit card, voucher, money order, or company check made payable to MWAA. Applicants no longer need to provide employment history documentation with their ID badge application.

All new air carrier (FAR Part 108) applicants requesting access to the SIDA must provide certification from their company that an FBI criminal history record check has been conducted. This certification will take the form of an FBI case number and certification official’s signature on a new ID badge application form. The Pass & ID Office cannot process the application form without this certification. Results of the record check is obtained usually in approximately three workdays. Questions may be addressed to the Pass & ID Office on (703) 417-8052.

Christopher U. Browne
Airport Manager
Ronald Reagan Washington National Airport
Section 1 – Applicant

THIS SECTION MUST BE TYPED

Last Name ___________________________ First Name ___________________________ Middle Name ___________________________

Social Security Number ___________________________ City/State/Zip ___________________________

Street Address ___________________________ Height ___________________________ Weight ___________________________ Gender ___________________________

Hair Color ___________________________ Eye Color ___________________________ Date of Birth ___________________________ Place of Birth ___________________________

Drivers License State ________ Drivers License Number ___________________________ Expiration Date ___________________________

Other Names Used ___________________________ (former name, nickname, maiden name)

Company Name ___________________________ Job Title ___________________________ Date of Hire ___________________________

Two forms of identification presented: 

AE yes 

1. Forgery of certificates, false marking of aircraft, and other aircraft registration violations AE No

2. Interference with air navigation AE Yes AE No

3. Improper transportation of a hazardous material AE Yes AE No

4. Aircraft piracy AE Yes AE No

5. Interference with flight crew members or flight attendants AE Yes AE No

6. Commission of certain crimes aboard aircraft in flight AE Yes AE No

7. Carrying a weapon or explosive aboard an aircraft AE Yes AE No

8. Conveying false information and threats AE Yes AE No

9. Aircraft piracy outside the special aircraft jurisdiction of the United States AE Yes AE No

10. Lighting violations involving transporting controlled substances AE Yes AE No

11. Unlawful entry into an aircraft or airport area that serves air carriers or foreign air carriers AE Yes AE No

contrary to established security requirements

12. Destruction of an aircraft or aircraft facility AE Yes AE No

13. Murder AE Yes AE No

14. Assault with intent to murder AE Yes AE No

15. Espionage AE Yes AE No

16. Sedition AE Yes AE No

17. Kidnapping or hostage taking AE Yes AE No

18. Treason AE Yes AE No

19. Rape or aggravated sexual abuse AE Yes AE No

20. Unlawful possession, use, sale, distribution, or manufacture of an explosive or weapon AE Yes AE No

21. Extortion AE Yes AE No

22. Armed or felony unarmed robbery AE Yes AE No

23. Distribution of, or intent to distribute, a controlled substance AE Yes AE No

24. Felony arson AE Yes AE No

25. A felony involving a threat AE Yes AE No

26. A felony involving willful destruction of property AE Yes AE No

27. A felony involving importation or manufacture of a controlled substance AE Yes AE No

28. A felony involving burglary AE Yes AE No

29. A felony involving theft AE Yes AE No

30. A felony involving dishonesty, fraud, or misrepresentation AE Yes AE No

31. A felony involving possession or distribution of stolen property AE Yes AE No

32. A felony involving aggravated assault AE Yes AE No

33. A felony involving bribery AE Yes AE No

34. A felony involving illegal possession of a controlled substance punishable by a maximum term of imprisonment of more than one year AE Yes AE No

35. Conspiracy or attempt to commit any of the aforementioned criminal acts AE Yes AE No

06/08/01
I understand that any individual who has been convicted or found not guilty by reason of insanity of the crimes listed on the reverse side within the previous ten years is legally prohibited from unescorted SIDA access.

I understand that I am required to report any future convictions brought against me that relate to the crimes listed on the reverse side. I understand that this application will be subject to an FBI criminal history record check and that I must provide fingerprints for the criminal history record check. All information obtained from the FBI criminal history record check will be kept confidential and used only for determining unescorted SIDA access. I understand that I am entitled to a copy of the FBI criminal history record check if I submit a written request to the Airport Security Coordinator. If I suspect that the criminal history record check is incorrect, I should contact the reporting agency directly and resubmit another application for verification. ________________________________ (initials)

**Applicant’s Security Responsibility Agreement**

1. I will not allow anyone else to use my ID badge or AOA access key.
2. I will wear my ID badge on my outermost garment at all times when in the restricted area.
3. I will challenge and report any individual who is not displaying an ID badge in the restricted area and report the incident to the Airport Operations Department or Airport Police.
4. I will ensure proper closing and locking of any AOA door or gate I used.
5. I will not allow anyone to follow me or my vehicle through any AOA door or gate.
6. I will report the theft or loss of my ID badge or key immediately to the Airport Operations Department.
7. I will report immediately any security violation I witness to the Airport Operations Department or Airport Police.

I have read the above security procedures and I understand that failure to comply with any of them may result in the revocation of my ID badge or key, which means that I will not be allowed access to the security controlled areas of the airport.

Applicant’s Signature _____________________________________________ Date Signed ___________________________

**Section III – Company Information and Certification**

Prime Contractor_________________________________________________________________________________________

Company Name ______________________________________________ Phone Number ____________________________

Street Address _______________________________________________ City/State/Zip _____________________________

Gate Agent Status?  Yes No AOA Gates ________________

AOA Motor Vehicle Operator Permit required?  Yes No

I understand that it is my company’s or agency’s responsibility to notify the Pass & ID Office or the Airport Operations Department immediately if an employee is terminated or loses his or her badge.

My company or agency will reimburse the Metropolitan Washington Airports Authority for any FAA fines levied against Ronald Reagan Washington National or Washington Dulles International Airports that are caused by an applicant’s failure to adhere to the Airport Security Program.

I certify that this applicant is currently employed by our company or agency.

Certification Official’s Name ________________________________ Title ___________________ Date _________________

Certification Official’s Signature _______________________________________

**Section IV – Air Carrier Criminal History Record Check Certification**

Name of Air Carrier _____________________________________________

I certify that an FBI criminal history record check has been conducted for _________________________________________ on __________________________ in accordance with Public Law #106-528.

(date)

The OPM case # is ________________________________________________ .

Certification Official’s Name ________________________________ Title ___________________ Date _________________

Certification Official’s Signature _______________________________________

**Section V – Security Trainer**

This applicant has completed SIDA training in accordance with the FAA approved curriculum cited in the Airport Security Program.

SIDA Trainer ______________________________ Signature ___________________________ Date _________________

**Section VI – AOA Motor Vehicle Operator Trainer**

This applicant has successfully completed the AOA Driver Training Class.

Driver Trainer ______________________________ Signature ___________________________ Date _________________

Driver's Test Score ____________________________ 060801
1. PURPOSE

This Airport Bulletin changes the fingerprint fees from $29 to $31, effective February 1, 2002.

2. DISTRIBUTION

This Bulletin is distributed to all Metropolitan Washington Airports Authority branches and above, air carriers, tenants, government, concessionaires, and contractors at DCA.

3. GENERAL

Effective December 23, 2000, FBI Criminal History Record Checks, using fingerprinting, are required for all new airport employees who are seeking unescorted access to the SIDA.

4. CHANGE

Effective February 1, 2002, the fingerprint fee is changed from $29 to $31 for each employee. This fee may be paid by cash, credit card, voucher, money order, or company check made payable to MWAA.

Questions may be addressed to the Airport Operations, Pass & ID Office on (703) 417-8052.

Christopher U. Browne
Airport Manager
Ronald Reagan Washington National Airport
Airport Advisory DCA 01/029

Subject: AOA Vehicle Gates

Dated November 6, 2001

2 Pages
Effective immediately, the only vehicle gates open for access on to the Air Operations Area (AOA) are Gate A and Gate D, located at the south end of the Airport.

**Gate A** is located on Thomas Avenue, adjacent to the south side of the Fuel Farm. Gate A operates 24 hours per day, seven days per week.

**Gate D** is located on Air Cargo Road, adjacent to the north side of the Fuel Farm and the south side of the Air Cargo Building. Gate D operates between 5:00 a.m. and 10:00 p.m., seven days per week.

Gate A and Gate D are the Airport's only designated (non-emergency) entry and inspection sites for any vehicles entering on to the AOA.

A. The requirements for vehicles and operators entering the AOA through Gate A and Gate D are as follows:

1. All personnel in the vehicle with a Security Identification Display Area (SIDA) / AOA ID badge shall present their badge(s) to the AOA Gate Guard for inspection. Only personnel with a valid SIDA / AOA ID badge will be granted unescorted entry on to the AOA.

2. All vehicles with a valid DCA AOA Inspection Decal and operated by personnel with a valid SIDA / AOA ID badge will be granted access on to the AOA without further vehicle inspection.

3. All vehicles without a DCA AOA Inspection Decal (except as noted in Section 5) shall be visually inspected by the AOA Gate Guard. Vehicle operators shall allow the AOA Gate Guard access to all areas of the vehicle for visual inspection purposes. Vehicles without a DCA AOA Inspection Decal may be allowed on to the AOA if escorted by a sponsor with a valid SIDA / AOA ID Badge in a DCA AOA authorized vehicle.

4. The AOA Gate Guard shall maintain a log of vehicles not displaying a current and valid DCA AOA Inspection Decal that enters on to the AOA. The log shall contain: vehicle operator, company name, sponsor name and their DCA AOA / SIDA ID badge number, destination on the AOA, and duration of stay.
5. The Authority's fire personnel displaying a valid employee-parking permit are exempt from a vehicle inspection when entering the AOA to park their privately owned vehicle (POV) at the Crash/Firehouse/Rescue facility. All fire personnel shall enter the AOA at Gate A or Gate D and shall present their AOA badge to the AOA Gate Guard before entering on to the AOA.

6. All vehicle operators, after entering on to the AOA, shall remain stopped until the AOA Gate has closed.

7. Vehicle operators entering the AOA through gates other than Gate A or Gate D for purposes other than responding to an emergency incident on the AOA are not authorized. Unauthorized use of any AOA Gate is cause for loss of AOA driving privileges.

B. Exemptions:

1. **Gate R**, located adjacent to the Authority's Corporate Office Building, is for Restricted Entry Only. Gate R shall not be used for routine exits from the AOA.

2. **All Authority Fire, Police, Operations, and a limited number of Authority Maintenance vehicles** may enter the AOA through any AOA vehicle gate only when in response to an emergency.

C. All vehicles are authorized to **EXIT** the AOA through any AOA vehicle gate, 24 hours per day, seven days per week, with the exception of Gate R (see Part B., Section 1., above).

*Please ensure that your staff is made aware of these security requirements.* If you have any questions or desire further clarification, please contact Mark Baldy on (703) 417-8050.
Part V

Department of Transportation

Federal Aviation Administration

14 CFR Parts 107 and 108
Unescorted Access Privilege; Final Rule
DEPARTMENT OF TRANSPORTATION

Federal Aviation Administration

14 CFR Parts 107 and 108

[Docket No. 26763; Amendment Nos. 107–7, 108–12]

RIN 2120–AE14

Unescorted Access Privilege

AGENCY: Federal Aviation Administration (FAA), DOT.

ACTION: Final rule.

SUMMARY: The FAA is issuing final regulations requiring airport operators and air carriers to conduct an employment investigation and disqualify individuals convicted of certain enumerated crimes from having, or being able to authorize others to have, unescorted access privileges to a security identification display area (SIDA) of a U.S. airport. This rule implements the employment investigation provisions of Section 105 of the Aviation Security Improvement Act of 1990. The rule will enhance the effectiveness of the U.S. civil aviation security system by ensuring that individuals applying for unescorted access privileges do not constitute an unreasonable risk to the security of the aviation system.

EFFECTIVE DATE: January 31, 1996.


SUPPLEMENTARY INFORMATION:

Availability of Document

Any person may obtain a copy of this document by submitting a request to the Federal Aviation Administration, Office of Public Affairs, Attention: Public Inquiry Center, APA–230, 800 Independence Avenue, SW., Washington, DC 20591, or by calling (202) 267–3484. Communications must identify the amendment number or docket number. Persons interested in being placed on a mailing list for future rules should also request a copy of Advisory Circular No. 11–2A, which describes the application procedures.

Background

Throughout the last decade, the FAA has recognized the need to investigate the backgrounds of individuals authorized to have unescorted access to security-restricted areas at U.S. airports. On November 26, 1985, the FAA amended airport and air carrier security programs to require 5-year background checks for individuals applying for unescorted access authority to the security controlled areas of an airport. The check requires the verification of such individual's employment history and references for the previous 5 years to the extent allowable by law. The December 21, 1988, destruction of Pan American World Airways Flight 103 by a terrorist bomb while in flight over Lockerbie, Scotland, was the worst disaster of its kind in U.S. civil aviation history. In response to this tragedy, on August 4, 1989, President Bush established the President's Commission on Aviation Security and Terrorism (Commission) (E.O. 12686) to assess the overall effectiveness of the U.S. civil aviation security system.

The Commission's May 15, 1990, report presented a series of recommendations intended to improve the U.S. civil aviation security system. The Commission originally recommended that Congress enact legislation requiring a criminal history records check for airport employees. The Commission further recommended that the legislation identify certain crimes that indicate a potential security risk, and enable airport operators to deny employment in positions requiring access to security sensitive areas on that basis. The Commission's recommendations formed the basis of the Aviation Security Improvement Act of 1990, Pub. L. 101–1064 (the Act). Section 105(a) of the Aviation Security Improvement Act (the Act) now codified as 49 U.S.C. 44936, added a new provision to the statute. This provision directs the FAA Administrator to promulgate regulations that subject individuals with unescorted access to U.S. or foreign air carrier aircraft, or to secured areas of U.S. airports serving air carriers, to such employment investigation provisions. In that proposal, the FAA Administrator determined necessary to ensure air transportation security.

The overwhelming majority of commenters supported FAA's proposal to require a criminal history records check for all individuals having unescorted access to the SIDA, and the proposal to require escorts for anyone inside the SIDA who did not have such a records check. Specifically, commenters argued that individuals with existing unescorted access privileges should be excluded from the criminal history records check requirement, and that the proposed escorting requirements were neither practical nor cost-effective. Some commenters questioned whether any benefit would result from requiring a criminal history check. Because of these concerns, commenters strongly recommended that the FAA exercise more flexibility in implementing the employment investigation provision of the Act.

Discussion of the SNPRM

In response to comments received during the public meetings and the FAA's re-evaluation of the NPRM, the FAA issued a supplemental notice of proposed rulemaking (SNPRM) (Notice No. 92–3; 57 FR 43294) on September 18, 1992. The SNPRM focused more broadly on the employment investigation process for individuals applying for unescorted access privilege. The SNPRM proposed an expanded employment application form, an enhanced 5-year employment history verification and, only where appropriate, a criminal history records check. Under this approach, a criminal history records check would be required only after the employment application process, including the history verification, "triggers" a need for one.
The proposed fingerprint-based criminal history records check process was similar to that proposed in the NPRM.

Discussion of SNPRM Comments

The FAA received 34 comments in response to the SNPRM. Commenters included Congressman James L. Oberstar, 12 airport operators, 3 air carriers, 2 individuals, 3 small businesses, 1 state transportation department, the Federal Bureau of Investigation, the U.S. Customs Service and the following aviation organizations: Air Transport Association (ATA), Air Transport Association of Canada (ATAc), Aircraft Owners and Pilots Association (AOPA), Airline Pilots Association (ALPA), Association of Airport Executives (AAAE), Association of Flight Attendants (AFA), Families of Pan Am 101/Lockerbier, National Association of Air Traffic Controllers (NATCA), Regional Airline Association (RAA).

Fifteen commenters support the employment investigation proposed in the SNPRM. Several of these commenters commend the FAA for its response and attention in addressing many of their major concerns in the initial notice.

Seven commenters oppose the proposal, arguing against the need for the employment investigation because no documented terrorist act has ever been committed by someone with both unescorted access privileges and a record of conviction for one of the disqualifying crimes listed in the Act. One commenter questions the link between past convictions for disqualifying crimes and future terrorist actions. Two commenters, a member of Congress and the Families of Pan Am 103/Lockerbier, want a more extensive employment investigation than that proposed in the SNPRM. They suggest extending the employment verification portion to 10 years and applying the employment investigation to individuals with existing unescorted access privilege.

Three commenters also discuss the degree of discretion provided the Administrator in implementing the employment investigation requirement of the Act. One commenter states that the Act does not require this regulation and the FAA should not issue a final rule. Another states that the Act requires only an employment investigation with a criminal history check as the Administrator determines necessary.

According to this commenter, issuance of a rule is completely discretionary. A third commenter contends that the statute mandates an employment investigation, not a criminal history records check. FAA Response: This rule enhances existing FAA security requirements and supports the objectives of the Act through a cost-effective and practical regulatory program. The FAA’s security requirements focus on protecting persons and property in air transportation against acts of criminal violence, air piracy, and terrorism. These acts are neither simple nor limited to sophisticated acts of international terrorists with political motives or acts of deranged individuals. Also of concern are individuals deliberately committing, or deliberately or unknowingly assisting in the commission of criminal acts against aviation for financial gain or reprisal. For example, individuals with a history of felony narcotics distribution may be more susceptible to exploitation by those wishing to target a passenger aircraft. In this scenario, the employee would willingly assist in placing a package of purported narcotics on the aircraft, only to find later that the packet actually contained an explosives device. A trust is placed in individuals authorized to have unescorted access, and it is reasonable to establish measures to reduce the likelihood that they will present a security risk to civil aviation.

The U.S. aviation industry has not experienced incidents in which there was a direct relation between the disqualifying offenses and a serious security incident, such as a terrorist bombing or hijacking. However, the Act indicates Congress’ concern that an individual’s criminal history could show a disposition to engage in such conduct in the future, which could result in a serious security incident. Moreover, it is a reasonable and feasible precaution to prohibit unescorted access to individuals with a criminal record for certain types of crimes. This rule uses practices similar to other industry standards (e.g., bankers, stockbrokers and employees at nuclear facilities).

The Act requires the FAA to issue regulations subjecting individuals with unescorted access to U.S. or foreign air carrier aircraft, or to SIDAs of U.S. airports, to such employment investigations, including a criminal history records check, as the Administrator determines necessary to ensure air transportation security. While the Act gives the Administrator flexibility in determining the employment investigation provision, the Congress clearly contemplated that granting unescorted access privileges would be tied to some type of employment investigation. In response to the public hearings and written comments, the FAA modified the initial proposal and developed the SNPRM to enhance aviation security in a more cost-effective manner. The FAA’s SNPRM stating:

The conferees have agreed to delete the language proposed by the House that would have prohibited the Federal Aviation Administration from implementing a rule to require criminal background checks of airline and airport employees. The conferees’ action is based on the Federal Aviation Administration’s Supplemental Notice of Proposed Rulemaking published in the September 18, 1992 Federal Register in which the Federal Aviation Administration revised an earlier proposed rulemaking. The conferees recognize that the Federal Aviation Administration has used its discretionary authority to address the many concerns raised by the industry groups about the operational, financial and constitutional issues associated with its earlier proposal, and have concurred that the Federal Aviation Administration should not be prohibited from moving forward with this approach.

This action clarified Congress’ view that the SNPRM conforms with the legislative intent of the Act.

Discussion of the Final Rule

The FAA developed this final rule based on the legislative mandate and the comments received during the rulemaking process. This rule amends 14 CFR parts 107 and 108; and parts 107 and 108 of the Federal Aviation Regulations (FAR). The rule expands the pre-existing requirements for an investigation into the background of individuals applying for unescorted access privileges to the SIDA of U.S. airports by providing specific guidelines for requirements.

The final rule augments and clarifies the process required to satisfactorily determine the eligibility of individuals for unescorted access privileges. This rule requires the employment investigation to include: provision of a 10-year employment history by those applying for access; verification of the most recent 5 years of that history by the employer; and the completion of a criminal history records check when specific conditions are identified as a result of the information obtained through the investigation process.

Similar in concept to the SNPRM, this final rule strengthens the existing employment investigation requirement by providing specific guidance on the type of information that must be
obtained and evaluated, identifying specific “triggers” that indicate a need to conduct a criminal history records check, and establishing recordkeeping requirements. This final rule differs from the SNPRM in that it requires individuals applying for unescorted access privileges to provide their employment history for a period of 10 years prior to the date of application rather than 5 years. While the employer will have to review the entire application, consistent with the SNPRM, only the most recent 5 years of this history need be verified as part of the employment investigation review. Hence, while an applicant will have to provide additional employment history information, this will not materially increase the burden on airport operators, air carriers or other non-air-carrier airport tenants involved in granting unescorted access privileges. The FAA believes that this approach increases the effectiveness of the rule in identifying individuals with unexplained gaps in employment who may have been convicted of the disqualifying crimes during the past 10 years and will afford employers additional information on which to base access determinations.

This final rule also modifies a key term used throughout the rule to further clarify its intent. Since it was used in the Act, the term “employment investigation” was used extensively in the NPRM and the SNPRM. While both notices specified that the “employment investigation” is related to access authority and not necessarily to employment, the final rule uses the term “access investigation.” The FAA believes that this term better describes the intent of the rule. The FAA Act of 1958 was recodified and appeared at 49 U.S.C. Subtitle VII, then under Public Law 103-272, effective July 5, 1994, recoding occurred under 49 U.S.C. Code “Transportation”. This Final Rule lists both the new statutory numbers for crimes committed and the former citations, in part because FBI records are likely to only have the latter citations.

Another modification to the SNPRM is that the FAA will act as the clearinghouse for criminal history records checks. The procedures for processing fingerprint cards and associated fees are discussed later in this preamble under § 107.31(i), “Fingerprint Processing.”

Further Action Considered

Although this final rule makes an important improvement to the civil aviation security system, and is fully consistent with the rulemaking record, the FAA is currently evaluating whether further changes may be warranted. Subsequent to the close of the comment period for the SNPRM, this country has experienced two major acts of domestic terrorism. The World Trade Center bombing and the recent bombing of a Federal office building in Oklahoma City are evidence of the threat of terrorism within the United States. While neither incident involved an aviation target or appears to have involved individuals who had a disqualifying criminal record that would have been disclosed by an FBI fingerprint check, the incidents to raise questions about whether a broader rule should be considered in light of the general level of threat. It also raises questions about whether the statutory authority should be expanded to include other persons with security responsibilities, such as checkpoint screeners, who do not necessarily have unescorted access to air carrier aircraft or to the secured area of an airport. However, the FAA has concluded that it is essential and appropriate to move forward with this final rule on the existing record and not further delay action until the FAA’s evaluation and possible further rulemaking are completed.

The FAA intends to actively consult with airport operators and air carriers as part of this evaluation. The effect of this rule and its actual implementation by airports and air carriers will be followed closely from the outset. In addition, input will be sought from the Aviation Security Advisory Committee. The FAA will determine what further actions may be necessary based on the evaluation. The FAA also will review intelligence information in relation to the possible impact of a more extensive criminal history check requirement.

Section-by-Section Analysis

Section 107.1 Applicability and Definitions

Escort

In the SNPRM, the FAA defined the term “escort” in § 107.1(b)(3). One commenter, NATA, states that the proposed definition of escort implies that this function and any associated responses must be performed by the same individual. NATA suggests that an individual other than the one performing the escort be allowed to perform follow-up actions, and that escorting by electronic means be allowed.

FAA Response: This rule retains the definition of “escort” that was included in the SNPRM, with minor modifications. Only an individual authorized by the airport operator to have access to areas controlled for security purposes may perform escorting. Specific action must be taken, in accordance with local airport procedures, if the individual under escort engages in activities other than those for which the escorted access is granted. The definition is modified by adding a sentence that explains that necessary responsive actions can be taken by the escort or other authorized individuals.

The definition of escort adopted in this rule includes a performance standard. The definition provides the latitude to use various methods and procedures for the escort as long as they meet the established standard. For example, an airport could choose to establish escorting procedures for its general aviation areas that use electronic means and prescribe specific follow-up actions.

Section 107.31 Access Investigation

Section 107.31(a)—Applicability

Area Covered

Six commenters to the SNPRM discuss the applicability of the regulation to the SIDA. RAA, ATA, and AOPA contend that at some airports broad SIDA definitions include the entire air operations areas (AOA). The commenters believe the FAA should mandate a consistently defined, limited SIDA.

An airport operator requests a broader applicability of the rule stating that two different levels of employment verification for SIDA and non-SIDA areas controlled for security purposes will be confusing. This operator recommends the rule apply uniformly to all areas that require identification badges. AACI and AAAE contend that one standard should apply to all, and they are particularly concerned that individuals performing air carrier screening are not included in the employment investigation rulemaking.

FAA Response: This rule applies only to airports that require continuous display of airport-approved identification, i.e., the SIDA as defined in § 107.25. The SIDA typically includes the secured area of an airport (§ 107.14 secured area) and some or all of the air operations areas (§ 107.13).

FAA guidance has defined the areas and types of operations for inclusion within the SIDA. Any expansion of an airport SIDA requires FAA approval. In such instances, application of the policy guidance assures uniformity to the extent practical. Given the varied operational areas at airports, it is not
The FAA has clarified that this rule does not apply to smaller airports that do not have a continuous display requirement by removing the reference to these airports contained in § 107.31(a)(2) of the SNPRM. However, if an airport has an area controlled for security reasons that is not a SIDA, the existing 5-year employment history verification continues to apply to individuals requesting unescorted access authority.

The access investigation requirement of this rule applies to individuals seeking unescorted access privileges in the SIDA as well as those in a position to authorize others to have such access and supersedes the 5-year employment history verification in the airport security program for the covered individuals. The issuance or denial of an identification credential for continuous display in the SIDA serves as the vehicle for implementation of this requirement from a practical and enforcement standpoint.

For individuals applying for positions that do not require SIDA unescorted access privileges (and thus are not covered by this rule), the existing security program language requiring the 5-year employment history verification will continue to apply. This includes security screening personnel and any other individuals with unescorted access only to security-controlled areas outside of a SIDA. While having somewhat different requirements may result in some extra administrative effort, the commenters did not provide any specific information showing that this will significantly increase the burden on airports. Except for the authority to access an applicant's criminal history record, an employer may use the application process specified in this rule in all circumstances.

Definition of Employer

One commenter points out that the SNPRM implies that all persons for whom an airport operator may authorize or deny unescorted access privileges are employees of the airport subject to being hired or fired by the airport operator. This commenter explains that many individuals applying for unescorted access privileges are not airport operator employees.

Two commenters address the consequences of the employment investigation proposed in the SNPRM on the employment process. One commenter states that the proposed employment investigation provision are intended to cover individuals with existing authority and individuals applying for unescorted access privilege. He argues that the existing 5-year employment history verification is not subject to FAA approval, and the FAA has not provided guidance on what constitutes an acceptable check. Therefore, Congressman Oberstar states that the final rule must “require that current employment investigation programs conform with those mandated in the final rule” and that “employers with non-conforming programs must be required to conduct 5-year employment checks of current employees to assure that they have undergone the same scrutiny as applicants.”

One commenter is uncertain whether individuals exempted under the proposal with a previous conviction for a disqualifying crime would lose their privileges for unescorted access.

FAA Response: While the Act gives the FAA authority to require employment investigations for individuals currently authorized for unescorted access privileges, the Act confers discretion on the FAA Administrator on methods for imposing such a requirement. Individuals authorized to have unescorted access privileges since November 26, 1985, have been subjected to a 5-year employment history verification required by the FAA in the security programs of airport operators and air carriers. Since granting these individuals unescorted access privileges, airport operators and air carriers have had the opportunity to observe the individual’s conduct.

The benefits, if any, of subjecting current employees with unescorted access authority to the proposed access investigation would not justify the disruption and cost that such a requirement would place on the air carriers and airport operators. The estimated cost for verifying employment histories of all existing employees would be an additional $5.4 million. Further, because of typically high turnover rates, much of the employee population with unescorted access will have been subjected to the expanded background check within a relatively short period. Therefore, the FAA concludes that air transportation security does not require the retroactive application of this rule to individuals with current unescorted access authority.

This rule does not require individuals currently authorized to have unescorted access privileges to disclose a past conviction for a disqualifying crime. However, if a conviction occurs after the effective date
of this rule, an individual with unescorted access authority will be subject to self-disclosure and disqualification from unescorted access privileges (see the Individual Accountability requirements of § 107.31(l) and § 108.33(h)).

120-Day Effective Date

Ten commenters address the timeframe between the final rule issuance date and the effective date the industry must begin to comply with the employee investigation requirements proposed in the SNPRM. Two commenters agree with the 90-day implementation period and seven commenters argue for a longer period of time. These commenters contend that additional time is needed for airport operators, air carriers, and airport tenants to set up the administrative procedures necessary to implement the rule, coordinate with other airports on rights to the 10-year budget and plan for required expenditures, and train personnel to implement the rule. Another states that an extended time period will prevent difficulties similar to those being experienced with the implementation of § 107.14. ATA suggests a period of six months to a year and another commenter proposes phasing in the regulation, starting with the Category X airports one year after the effective date. AACI and AAAE recommend that the effective date, rather than the Federal Register publication date, be used to exclude individuals holding existing unescorted access privileges from the employment investigation requirements.

FAA Response: The affected parties have been provided ample opportunities to comment on the implementation of Section 105 of the Act through ASAC recommendations, and in response to the NPRM (for which the comment period was extended), three public meetings, and the revised proposal in the SNPRM. The access investigation requirements of this rule should not place an excessive administrative burden on airport operators and air carriers. The requirement to modify the existing 5-year employment history verification and establish a procedure to conduct a criminal history records check, where necessary, utilizes many existing practices and procedures. However, as this rule will affect a wide spectrum of airport tenants, and in hopes of ensuring a smooth and orderly transition to the new procedures, the FAA is making the rule effective 120 days after publication in the Federal Register.

Section 107.31(b)—Access Investigation Requirements

Coverage of Access Investigation

Of the 15 commenters responding on this issue, 13 concur with the FAA’s proposal to use the 5-year rather than a 10-year employment history verification as the primary screening procedure. The commenters supporting the 5-year verification argue that covering more than 5 years would produce less useful information because it would be difficult to find previous employers to provide reliable references, require more staff and take a longer time to complete, resulting in additional costs. According to these commenters, the expanded application form, which includes the applicant’s certification as to prior criminal convictions, coupled with the enhanced 5-year verification is sufficient to alert management of a need for further investigation. One air carrier comments that it currently requires applicants to provide 10 years of employment information, although it only verifies the previous 5 years.

The two commenters opposing the 5-year employment verification, Congressman Oberstar and the Families of Pan Am 103, believe that it will not reveal convictions that may have occurred in the previous 10 years and that the proposal does not comply with the Act.

FAA Response: At the SNPRM stage, the FAA considered increasing the employment history verification from 5 years to 10 years. It determined that to do so would increase the costs and time spent on the verification without appreciably enhancing aviation security. This could result in triggering relatively few additional records checks, but at an additional cost of at least $5.50 per access investigation or about $9 million over the next decade. However, as a result of the comments, the FAA carefully reviewed the 10-year employment history issue. The FAA determined that it would be useful and reasonable to require individual applicants to provide a 10-year employment history. The additional information will increase the likelihood of identifying 12-month employment gaps and provide an additional decision tool to employers.

Under the rule, airport operators, air carriers and other non-air-carrier airport tenants are required to verify only the most recent 5 years. However, employment gaps of more than 12 months must be resolved for the entire 10-year period if a records check is accomplished. From a practical viewpoint, the verification of an individual’s 5-year employment history provides an accurate indicator of the individual’s background and of the overall veracity of the information provided by the applicant on the form. However, the additional employment history information available to the employer enhances the 5-year verification portion and increases the deterrent value of the application process. Applicants planning to fabricate employment history information will be faced with twice the challenge and their chance of discovery will thus be increased. Truthful applicants will identify employment gaps that require further evaluation.

The 10-year period is also covered by requiring the applicant to list on the application convictions occurring in the past 10 years for any disqualifying crimes. The application form also must notify individuals that they will be subject to an employment history verification and possibly an FBI criminal history records check.

Individuals who are subject to a criminal history records check would be disqualified if their record discloses a conviction for any of the listed crimes in the previous 10 years.

Because the disqualifying crimes are serious felonies, an arrest, conviction, and incarceration would normally show up as a gap in the individual’s employment history, thus triggering a criminal history records check. The requirement to conduct a criminal history records check should help discourage anyone with a conviction for one of the disqualifying crimes from applying for a position requiring unescorted access authority.

Convictions for Disqualifying Crimes

Twelve commenters discuss the list of convictions for disqualifying crimes. Three of the commenters specifically agree that arson should be a disqualifying crime, as the FAA proposed in the SNPRM. AACI and AAAE oppose having arson included as a disqualifying crime. These organizations argue that, in their view, there is no significant history of arson occurring on an airport ramp.

Ten commenters support disqualifying from unescorted access privileges a person found not guilty by reason of insanity for any of the disqualifying crimes. Some of the commenters argue that insanity is not a crime and, therefore, some form of rehabilitation should be allowed. As an example, the commenters refer to the State of California system that requires that a person found not guilty by reason of insanity must be certified as rehabilitated by a court before the individual’s rights are restored. ATA
points out that, in accordance with its reading of the Act and the Americans with Disability Act, the FAA has the legal authority and right to include insanity as a disqualifying factor. Another commenter states that insanity as a disqualifying factor should be determined on a case-by-case basis and that the final determination should be based on national and local FAA field office guidelines to ensure nationwide consistency.

AAACI and AAACE state that “certain crimes aboard aircraft in flight” is too vague and that this disqualifying crime needs to be better explained. They are also concerned that the regulation would not permit an employer to take into account the ten years for purposes of allowing unescorted access.

Three commenters state that the regulation should not limit the employer to those crimes on the list. In their view, an employer should have some discretion to include other crimes or conditions as disqualifying.

Two commenters assert there should be measures for punishing applicants who falsify the information they provide on the application forms or, at a minimum, disqualifying the individual from unescorted access. One of these commenters states that individuals convicted of any of the disqualifying crimes would not hesitate to falsify an application form and that stronger measures are needed, such as making it a Federal crime to falsify such information.

FAA Response: As proposed, this rule adds felony arson to the list of disqualifying crimes. (In the SNPRM, FAA proposed “arson”; the rationale for the clarifying change can be found below.) The deliberate nature of the offense and the safety and practical considerations of providing fuel make it logical to do so. Although the FAA is not aware of any instance where an individual with unescorted access privileges ever perpetrated an act of arson at an airport, arson has occurred at airports and is too dangerous an act to omit it from the list of disqualifying crimes.

Also, in response to comments received on the initial notice and the SNPRM, this rule adds “not guilty by reason of insanity” for any of the disqualifying crimes as a disqualifying factor. While recognizing that insanity is not a crime, the FAA concludes that insanity associated with a disqualifying crime should be a disqualifying condition because of the seriousness of these crimes and the difficulty involved in ascertaining recovery.

The FAA has made some minor clarifying changes to the introductory language of § 107.31(b). The phrase “in any jurisdiction” has been added to parallel the language of the Act. Also added is the phrase “a crime involving * * *” to the enumerated offenses in order to make clear that the intent of the rule is to disqualify an individual who has been convicted of one of the disqualifying offenses, even if the name of the statute under which the individual was convicted does not exactly match the language of the final rule. As long as the conviction involves a crime specified in the rule, the individual would be disqualified.

In its comment to the NPRM, the Department of Justice’s Criminal Division requested several changes to the rule language to which the FAA has agreed. The Division suggested that we limit disqualifying convictions for arson to felony arson in order to exclude instances of minor eruptions. The Division also requested that some of the disqualifying offenses be further defined. These revisions include:

• § 107.31(b)(2)(xvii): the phrase “or hostage taking” has been added after “kiddnapping”;
• § 107.31(b)(2)(x): the phrase “or aggravated sexual abuse” has been added after “rape”;
• § 107.31(b)(2)(xx): the word “use” has been added before “sale.”

It is the FAA’s understanding and intent that these changes clarify the extent of Congress but do not substantively expand the list of disqualifying crimes. The Criminal Division also requested that § 107.31(b)(2)(xxv) be revised to include “attempts” to commit any of the aforementioned criminal acts. The Division states that while this section, as proposed, included a conviction for conspiracy to commit any of the enumerated offenses (as required by the Act), the conduct underlying an attempt may be more serious than that required to support a conviction of conspiracy. The FAA has therefore revised this section to include the phrase “or attempt.”

The Act provides no discretion for rehabilitation, requiring only a 10-year period from the time of the conviction for the disqualifying offense. This rule also includes the 10-year period for instances of not guilty by reason of insanity.

In the rule, the FAA does not attempt to further define the commission of “certain crimes aboard aircraft” because it is one of the named disqualifying crimes from the Act. An individual’s criminal record would reflect convictions for this offense as a specific violation listed in 49 U.S.C. 46506.

This rule limits the mandatory disqualifying crimes to those required by the statute and the additional disqualifiers discussed above. Apart from meeting the requirements of this rule for unescorted access privileges, an airport operator and air carrier will retain discretion to determine the suitability and qualifications of applicants for unescorted access privileges based on any other information available to them.

This rule does not include penalties for falsifying application information. It is not a disqualifying condition covered by the Act, and the decision to deny access based upon falsification would be a local determination. However, substantial inconsistencies between required information provided on the application and information obtained during the access investigation would trigger a criminal history records check.

If the access investigation discloses a conviction for a disqualifying crime in the previous 10 years measured from the date the verification is initiated, the individual may not be granted unescorted access authority. The Act does not allow the consideration of the possible rehabilitation of an individual.

The disqualifying crimes identified in this rule include specific sections of 49 U.S.C. Chapters 463 and 465, sections of the United States Criminal Code, offenses named in the Act, and two additional disqualifiers.

The specific sections of 49 U.S.C. Chapters 463 and 465 are: (b) § 46706 forgery of certificates, false marking of aircraft and other aircraft registration violations; (c) § 46308 interference with air navigation; (h) § 46312 improper transportation of a hazardous material; (i) § 46502 aircraft piracy; (j) § 46504 interference with flightcrew members or flight attendants; (k) § 46506 commission of certain crimes aboard aircraft in flight; (l) § 46505 carrying a weapon or explosives aboard an aircraft; (m) § 46507 conveying false information and threats; (n) § 46502(b) aircraft piracy outside the special aircraft jurisdiction of the United States; (a) § 46315 lighting violations involving transporting controlled substances; and (r) § 46314 unlawful entry into an aircraft or airport area that serves air carriers or foreign air carriers contrary to established security requirements.

The disqualifying crime in 18 U.S.C. 32 is the destruction of an aircraft or aircraft facility.

The other disqualifying crimes are: murder; assault with intent to murder;
Espionage: sedition; kidnapping or hostage taking; treason; rape or aggravated sexual abuse; unlawful possession, use, sale, distribution, or manufacture of an explosive or weapon; extortion; armed robbery; distribution of, or intent to distribute, a controlled substance; felony arson; conspiracy or attempt to commit any of these criminal acts; or a finding of not guilty by reason of insanity for any of these criminal acts.

This rule does not limit the ability of airport operators and air carriers to review an individual's complete FBI criminal history record, although the record may not be requested unless one of the regulatory triggers is met. However, any decision to deny unescorted access may be attributed to this rule only if it is based on the individual's conviction within the previous 10 years of an enumerated crime. Any other adverse information contained in the criminal record does not disqualify an individual under this rule.

Section 107.31(c)—Elements of Access Investigations

Employment History Verification

A number of commenters support the process for conducting the verification outlined in the SNPRM. In the SNPRM, the FAA proposed that applicants be required to prove their identity by providing two forms of identification (ID), including a photo ID. In the SNPRM, the FAA proposed that applicants would have to explain employment gaps of more than 12 months in the previous 5 years, and that employers would have to verify information on the application for unescorted access in writing, by telephone, or in person. The FAA solicited comments on whether other means of verifying an individual's employment, such as written documentation, should be acceptable in the verification process.

Two commenters specifically support accepting documentation instead of telephone calls or visits to previous employers. One commenter suggests that legitimate gaps in employment can be documented by copies of school records or certified letters of references from physicians, clergy, or other professionals. Two commenters caution that the rule could have the unintended consequence of generating greater paperwork burdens on employers who must keep records of how they verified employment. A nether commenter opposes adding security-related information requirements to its application forms, fearing that such forms could become needlessly lengthy.

FAA Response: This rule specifies the information required on the application, requires proof of the individual's identity, and requires verification of representations made by the individual. The FAA has crafted the rule using existing industry procedures and practices where possible to avoid creating unnecessary paperwork burdens. The individual applying for unescorted access privileges must complete an application form that includes: (1) the individual's full name, as well as any aliases or nicknames; (2) the dates, names, phone numbers, and addresses of the individual's previous employers for the last 10 years, with explanations for any gaps in employment of more than 12 months; (3) a notice that the individual will be subject to an employment history verification and possibly a criminal history records check; and (4) a question asking if the individual has been convicted of any of the disqualifying crimes or conditions during the previous 10 years. To assist the applicant in understanding the question on convictions, it would be advisable for the application to include a list of the disqualifying crimes or conditions. This rule permits supplementing an existing application form with a separate sheet requesting the required information and questions.

The information on the application will help identify applicants who may have a disqualifying conviction. For example, an unexplained gap in employment may have occurred due to incarceration for a conviction of a disqualifying crime. The airport operator is responsible for verifying, or accepting certification that the information required on the employment application was verified, to the extent necessary, to validate representations made regarding the most recent 5-year period. This process is similar to that used for the existing 5-year employment verification conducted by telephone, in writing, or in person. This rule allows the use of documentation to verify an individual's previous employment history. However, it is important for airport operators and air carriers to carefully examine the documentation provided to guard against counterfeit documentation.

In cases where a previous employer has gone out of business, a reasonable attempt to verify the period of prior employment should be made. Pay stubs, tax records, or other documentation records be used to support those statements on the application.

Section 107.31(n) requires maintaining a record of the method used to verify the applicant's most recent 5 years of employment and the results obtained. Section 107.31(n) also discusses the specific recordkeeping requirements.

Conditions Requiring a Criminal History Records Check

Four commenters address the conditions that "trigger" the requirement for an FBI criminal history records check. One commenter fully supports the triggers proposed in the SNPRM although it requests that the triggers not be considered as limitations. This commenter suggests that an airport operator or air carrier could elect to conduct a complete criminal history records check if, for example, it found an unexplained gap in employment of less than 12 months. Another commenter questions the adequacy of a 12-month period asserting that a person could serve less than 12 months for a disqualifying crime or could be allowed to plead guilty to a lesser crime.

AACI and AAIE believe that two of the conditions triggering a check are virtually identical to each other. These are: (1) the individual is unable to support statements made or there are significant inconsistencies between information provided on the application in response to questions required by the rule and that which is obtained through the verification process; and (2) information becomes available during the employment history verification indicating a possible conviction for one of the disqualifying crimes.

FAA Response: If one or more of the conditions or "triggers" established by the rule is activated, a fingerprint-based check of the criminal records maintained by the FBI must be completed prior to determining if unescorted access authority will be granted. An airport operator or air carrier is not permitted to establish additional triggers for requesting a criminal check under the authority provided by this rule.

The Act provides the statutory authority for airport operators and air carriers to access FBI records. The Act has been implemented by these regulations, which limit the circumstances under which the airport operator or air carrier can get the criminal history record. However, on its own authority, a potential employer could disqualify someone from unescorted access authority or refuse to hire an individual for an unexplained gap in employment of less than 12 months, or for any other reason. Of course, these actions would have to be
consistent with other applicable laws. Also under its own authority, an employer could apply the employment verification (but not the FBI criminal history records check), to any employees, not just those covered by this rule.

The “triggers” or conditions for the criminal history records check are based on information supplied by the aviation industry on the criteria used by some air carriers to screen job applicants. The combination of triggers provides the appropriate conditions to trigger the requirement for further review of the individual’s background through a criminal history records check.

Under the first trigger, an individual who is not able to adequately account for 12 months or more of unemployment over the past 10 years in a manner that substantiates that he or she was not incarcerated for a disqualifying crime would be subject to a criminal history records check. Note that while there is no requirement to verify the information in an applicant’s employment history for years 6 to 10, there is an obligation to resolve periods of unemployment of more than 12 months. Unemployment for a 12-month period or more does not automatically trigger a check. Rather, the criminal check is required when the period of unemployment cannot be verified through the checking of appropriate documentation or references. For example, a gap can be satisfactorily explained by receipts for unemployment compensation, travel records, or other information providing sufficient evidence of an individual’s whereabouts. In instances where an individual was self-employed, tax records, billing records, work orders or other means can be used to support the claims made on the application.

Second, a criminal history records check is triggered if there is an inability to substantiate statements made, or if there are significant inconsistencies between the information provided by the applicant or the information obtained during the employment verification requirement is intentionally defined using broad terms to allow the airport operator and employer to determine what is acceptable. However, if an individual’s employment cannot be verified, this is considered an inability to substantiate statements made.

Third, if information becomes available during the course of the access investigation indicating a possible conviction for one of the disqualifying crimes, a criminal history records check is required.

Responding to the question raised by AAIC and AAAE, there is a significant difference between finding out during the access investigation process that information provided was not correct versus finding information that indicates the individual may have a conviction for a disqualifying crime. If incorrect information is provided, it does not necessarily indicate the presence of a disqualifying conviction that raises questions about the individual’s truthfulness. An individual’s truthfulness is a key component of the access investigation process. Lack of veracity suggest the need to investigate further to determine if the person is trying to conceal a conviction for a disqualifying crime.

The purpose of the last trigger is to identify individuals that may require a criminal check based on any positive information identified during the access investigation. The trigger is intended to substantiate information provided. Section 107.31(d)—Escorted Access

Under §107.31(d) of the SNPRM, an individual who does not have unescorted access privileges may be permitted to enter a security area under escort. Five commenters object to allowing an individual who is the subject of a criminal history investigation access to a secured area even under escort because an on-going investigation indicates the likelihood of a criminal record. Three commenters also believe that the escort language proposed in §107.31(d) of SNPRM is inconsistent with the FAA’s policy in §107.14.

FAA Response: This rule requires individuals who have not been authorized to have unescorted access authority to be under escort, as defined in §107.11(b)(3), while the SIDA. The employer retains the option of completing the access investigation prior to hiring an individual needing unescorted access privileges rather than providing an escort while the investigation is pending. The primary means of determining an individual’s eligibility for unescorted access is the employment history verification, which normally takes from 5 to 10 days to complete. Thus, escorting is not necessary for most individuals while undergoing the check because the applicants would not be employed in a position whose utility is predicated on unescorted access until completion of the employment history verification.

The primary reason for security access under this rule is for individuals awaiting a criminal history records check. Escorted access is permissible while in the security sensitive area even though a criminal history records check has been triggered. A criminal history records check may take from 30 to 90 days to complete; escorted access is allowable when the employment history verification triggers one of the conditions requiring a criminal check. There is nothing in the rule language that requires an airport operator to provide escorted access into a SIDA to an individual undergoing a criminal history records check.

Under the FAA’s policy on §107.14(a) access controls, an individual with §107.14(a) access privileges may not be escorted through an access point meeting the requirements of §107.14. Each person with §107.14(a) access must be subjected to the access control system. Because §107.31(d) is applicable only to individuals not authorized for unescorted access, the escort language in this section is consistent with the FAA’s policy on §107.14.

Section 107.31(e)—Exceptions to the Investigation Requirements

Six commenters respond to the proposed exceptions from the employment investigation included in the SNPRM. The exceptions included Federal, State, and local government employees who as a condition of employment have been subject to an employment investigation; crew members of foreign air carriers covered by alternate security arrangements; individuals who have been continuously employed in a position requiring unescorted access by another airport operator, tenant, or air carrier; and individuals who have been authorized access to the U.S. Customs Service security area of an airport.

Under this rule, certain categories of individuals are excluded from the access investigation requirement. The FAA expects each airport operator to develop the procedures it uses to implement this section and, where appropriate, issue the individual identification media indicating authorization for unescorted access privileges.

Government Employees

Two commenters request selective application of the exception for Federal, State, and local government employees because employment verification by different entities may not be as stringent as that proposed in the SNPRM. The commenters also raise concerns over the issue of Federal and local law enforcement officers observing the airport’s access rules and requirements. Another commenter wants to ensure that the final rule does not alter the
access authority of FAA Safety Inspectors using Form 8000–39.

FAA Response: This rule adopts the language proposed in the SNPRM that no additional investigation is required for Federal, state, and local government employees who have been subjected to an employment investigation by their respective agencies. Typically, the government employer subjects applicants to an employment investigation that is at least equivalent to that proposed in this rule. For example, both Standard Form 171 and Optional Form 306 requires Federal applicants to disclose convictions, and the Office of Personnel Management, where appropriate, conducts a criminal history records check. The rule also provides an option to except state and local governments. This exception will reduce the cost and burden of implementing this rule, while maintaining an effective level of security. Airport operators should work with representatives from the Federal, state and local government agencies to resolve the type of biographical information needed to receive the identification media.

With regard to using Form 8000–39, this rule will not have any effect. Form 8000–39 will continue to authorize the FAA Inspectors to be present in an air operations areas to conduct short term duties associated with their safety related responsibilities.

Foreign Air Carrier Employees

Five commenters address the application of the employment investigation to employees of foreign air carriers. ATA believes the alternate security arrangement for foreign air carrier flightcrew members included in the SNPRM creates “serious competitive imbalances between U.S. and foreign carriers.” ATA implies that the advantage would be to the foreign carriers.

ATAC states that it does not object to the requirement to conduct employment investigations for individuals employed by Canadian carriers in the U.S. applying for unescorted access. However, ATAC contends that the alternative program for transient air crews is unnecessary because Canadian carriers already subject their air crews to a “criminal/subversive/financial security check” before a Transport Canada Airside Restricted Area Pass to operate from Canadian airports is granted. ATAC argues that this security check is more effective than the employment investigation requirement in the SNPRM and that the FAA should, therefore, allow Canadian air crews unrestricted access in U.S. airports or at least to areas and offices necessary for operational functions.

A foreign air carrier raises several concerns. The first is related to section 105(a) of the Act which states: “Nothing in this subsection shall be construed as requiring investigations or record checks where such investigations or record checks are prohibited by applicable laws of a foreign government.”

This commenter states that the investigation of employees hired in another country and assigned to duty in the U.S. could require an investigation of records in some other country where privacy laws prohibit such an investigation. The commenter recommends addressing this conflict in the rule by stating that such investigations be performed only to the extent permitted by law in the foreign country.

This foreign air carrier requests that the alternate security procedures be expanded to include all flightcrew members and to areas beyond the footprints of the aircraft. The preamble to the SNPRM explained an example of an alternate system as language in the airport security program permitting a foreign air carrier flightcrew member to have unescorted access or movement limited to the footprints of their aircraft. The commenter asks that the FAA’s final rule explicitly require airport operators to consult with foreign air carriers to identify areas to which crew members need access using the alternate security arrangement.

This carrier also suggests that the SNPRM be revised to allow foreign air carriers to use temporary personnel without performing an employment investigation. According to the commenter, these personnel could be subject to alternate security arrangements, specified in an airport operator security program, restricting access of such personnel to the areas necessary for performance of their jobs. The carrier contends that the revision is needed because foreign air carriers often require services of special relief personnel at particular airports for brief periods. The commenter believes that temporary duty assignments are vital to foreign air carriers, which have significantly fewer permanent personnel. In addition, the commenter believes that investigations by foreign countries for foreign air carrier flightcrew members would be limited to foreign flightcrew members (i.e., captain, second-in-command, flight engineer, or company check pilot) in the immediate vicinity of the aircraft to which they are assigned. The FAA is willing to consider the merits of including cabin crew and expanding the scope of ramp movement for foreign air carrier crew members on a case-by-case basis. Any alternate arrangements should be developed with and coordinated through the airport operator.

Responding to the concerns raised by ATA over the proposed authority to permit alternate arrangements for foreign crew members, the FAA has determined that it is reasonable from a security standpoint, and consistent with international practices, to permit limited access (around the assigned aircraft). Failure to provide alternate procedures for foreign air carrier crews could result in the adoption of additional requirements for investigations by foreign countries for U.S. air carrier personnel. There are significant operational restrictions associated with using the alternate arrangement that may accrue to a foreign air carrier. In addition, there is a very low probability of detecting disqualifying convictions for a foreign national based outside the U.S. through an investigation of FBI records because those records normally include only arrests and convictions occurring in the U.S.

This rule does not specifically allow for the acceptance of the Transport Canada Airside Restricted Area Pass as meeting the alternate arrangement. However, the required access investigation is more easily
accomplished for Canadian flightcrew members as a result of that country’s program. The approach of the Canadian system, or similar systems in use by other countries, could result in the facilitation of using documentary evidence of employment verification.

The FAA agrees that the Act limits employment investigations to the extent allowable by the law in the foreign country. However, if the employment history verification or other aspects of the access investigation could not be completed as a result of another country’s law, this would trigger a need to conduct the criminal history records check.

The problem of temporary employees is not specific or limited to foreign carriers. This rule would apply to any individual applying for unescorted access privileges. Considering the short period of time it takes to perform the employment history verification portion of the access investigation (which would authorize most individuals for unescorted access authority), the FAA contends this is not an unreasonable requirement; moreover, if the assignment is of short duration, escorting may be the simplest solution.

Transfer of Privilege

Two commenters believe that an individual who has been continuously employed by an air carrier, airport operator, or non-air-carrier tenant should be authorized unescorted access without having to be continuously employed in a position requiring unescorted access. Another commenter recommends that the FAA implement a uniform process for accepting transfers of individuals, so that there will be nationwide consistency in applying this provision. ATA expresses concern that the authority to grant unescorted access privileges to an individual transferring unescorted access privileges to an individual transferring an airport operator, or non-air-carrier tenant shall be the responsibility of the FAA that the authority for unescorted access must be granted at the FAA’s discretion. ATA notes that in the SNPRM the FAA contended that the requirement is not unreasonable; moreover, if the assignment is of short duration, escorting may be the simplest solution.

Individuals Subject To Investigation By Customs

One commenter suggests that the FAA coordinate with the U.S. Customs Service on its pending access rule for Customs Service security areas of an airport. The commenter’s concerns focus on the effect on operations, costs, and possible duplication of the two rules.

FAA Response: This rule permits an airport operator to accept the background checks performed by the U.S. Customs Service to meet the FAA’s access investigation requirement. Accepting the background investigation by Customs avoids a redundant check, because many of these contractors serve the FAA security program. The FAA also agrees that the responsibility for criminal history records checks of their contractors should be the responsibility of the airport operator.

FAA Response: This final rule adopts the procedures proposed in the SNPRM for accepting air carrier access investigations and non-air-carrier tenant employment history verifications. The rule does not attempt to establish uniform procedures for accepting transfers; rather, the rule sets the minimum requirement for continuous access to the FAA training. Under § 107.25 and associated FAA policy, individuals who have been subject to SIDA training who subsequently transfer their unescorted access must receive site-specific SIDA training at the new airport.

Individuals Subject To Investigation By Customs

One commenter suggests that the FAA coordinate with the U.S. Customs Service on its pending access rule for Customs Service security areas of an airport. The commenter’s concerns focus on the effect on operations, costs, and possible duplication of the two rules.

FAA Response: This rule permits an airport operator to accept the background checks performed by the U.S. Customs Service to meet the FAA’s access investigation requirement. Accepting the background investigation by Customs avoids a redundant check, because many of these contractors serve the FAA security program. The FAA also agrees that the responsibility for criminal history records checks of their contractors should be the responsibility of the airport operator.

FAA Response: This final rule adopts the procedures proposed in the SNPRM for accepting air carrier access investigations and non-air-carrier tenant employment history verifications. The rule does not attempt to establish uniform procedures for accepting transfers; rather, the rule sets the minimum requirement for continuous access to the FAA training. Under § 107.25 and associated FAA policy, individuals who have been subject to SIDA training who subsequently transfer their unescorted access must receive site-specific SIDA training at the new airport.

Individuals Subject To Investigation By Customs

One commenter suggests that the FAA coordinate with the U.S. Customs Service on its pending access rule for Customs Service security areas of an airport. The commenter’s concerns focus on the effect on operations, costs, and possible duplication of the two rules.

FAA Response: This rule permits an airport operator to accept the background checks performed by the U.S. Customs Service to meet the FAA’s access investigation requirement. Accepting the background investigation by Customs avoids a redundant check, because many of these contractors serve the FAA security program. The FAA also agrees that the responsibility for criminal history records checks of their contractors should be the responsibility of the airport operator.

FAA Response: This final rule adopts the procedures proposed in the SNPRM for accepting air carrier access investigations and non-air-carrier tenant employment history verifications. The rule does not attempt to establish uniform procedures for accepting transfers; rather, the rule sets the minimum requirement for continuous access to the FAA training. Under § 107.25 and associated FAA policy, individuals who have been subject to SIDA training who subsequently transfer their unescorted access must receive site-specific SIDA training at the new airport.

Individuals Subject To Investigation By Customs

One commenter suggests that the FAA coordinate with the U.S. Customs Service on its pending access rule for Customs Service security areas of an airport. The commenter’s concerns focus on the effect on operations, costs, and possible duplication of the two rules.

FAA Response: This rule permits an airport operator to accept the background checks performed by the U.S. Customs Service to meet the FAA’s access investigation requirement. Accepting the background investigation by Customs avoids a redundant check, because many of these contractors serve the FAA security program. The FAA also agrees that the responsibility for criminal history records checks of their contractors should be the responsibility of the airport operator.

FAA Response: This final rule adopts the procedures proposed in the SNPRM for accepting air carrier access investigations and non-air-carrier tenant employment history verifications. The rule does not attempt to establish uniform procedures for accepting transfers; rather, the rule sets the minimum requirement for continuous access to the FAA training. Under § 107.25 and associated FAA policy, individuals who have been subject to SIDA training who subsequently transfer their unescorted access must receive site-specific SIDA training at the new airport.

Individuals Subject To Investigation By Customs

One commenter suggests that the FAA coordinate with the U.S. Customs Service on its pending access rule for Customs Service security areas of an airport. The commenter’s concerns focus on the effect on operations, costs, and possible duplication of the two rules.

FAA Response: This rule permits an airport operator to accept the background checks performed by the U.S. Customs Service to meet the FAA’s access investigation requirement. Accepting the background investigation by Customs avoids a redundant check, because many of these contractors serve the FAA security program. The FAA also agrees that the responsibility for criminal history records checks of their contractors should be the responsibility of the airport operator.

FAA Response: This final rule adopts the procedures proposed in the SNPRM for accepting air carrier access investigations and non-air-carrier tenant employment history verifications. The rule does not attempt to establish uniform procedures for accepting transfers; rather, the rule sets the minimum requirement for continuous access to the FAA training. Under § 107.25 and associated FAA policy, individuals who have been subject to SIDA training who subsequently transfer their unescorted access must receive site-specific SIDA training at the new airport.

Individuals Subject To Investigation By Customs

One commenter suggests that the FAA coordinate with the U.S. Customs Service on its pending access rule for Customs Service security areas of an airport. The commenter’s concerns focus on the effect on operations, costs, and possible duplication of the two rules.

FAA Response: This rule permits an airport operator to accept the background checks performed by the U.S. Customs Service to meet the FAA’s access investigation requirement. Accepting the background investigation by Customs avoids a redundant check, because many of these contractors serve the FAA security program. The FAA also agrees that the responsibility for criminal history records checks of their contractors should be the responsibility of the airport operator.

FAA Response: This final rule adopts the procedures proposed in the SNPRM for accepting air carrier access investigations and non-air-carrier tenant employment history verifications. The rule does not attempt to establish uniform procedures for accepting transfers; rather, the rule sets the minimum requirement for continuous access to the FAA training. Under § 107.25 and associated FAA policy, individuals who have been subject to SIDA training who subsequently transfer their unescorted access must receive site-specific SIDA training at the new airport.

Individuals Subject To Investigation By Customs

One commenter suggests that the FAA coordinate with the U.S. Customs Service on its pending access rule for Customs Service security areas of an airport. The commenter’s concerns focus on the effect on operations, costs, and possible duplication of the two rules.

FAA Response: This rule permits an airport operator to accept the background checks performed by the U.S. Customs Service to meet the FAA’s access investigation requirement. Accepting the background investigation by Customs avoids a redundant check, because many of these contractors serve the FAA security program. The FAA also agrees that the responsibility for criminal history records checks of their contractors should be the responsibility of the airport operator.

FAA Response: This final rule adopts the procedures proposed in the SNPRM for accepting air carrier access investigations and non-air-carrier tenant employment history verifications. The rule does not attempt to establish uniform procedures for accepting transfers; rather, the rule sets the minimum requirement for continuous access to the FAA training. Under § 107.25 and associated FAA policy, individuals who have been subject to SIDA training who subsequently transfer their unescorted access must receive site-specific SIDA training at the new airport.

Individuals Subject To Investigation By Customs

One commenter suggests that the FAA coordinate with the U.S. Customs Service on its pending access rule for Customs Service security areas of an airport. The commenter’s concerns focus on the effect on operations, costs, and possible duplication of the two rules.

FAA Response: This rule permits an airport operator to accept the background checks performed by the U.S. Customs Service to meet the FAA’s access investigation requirement. Accepting the background investigation by Customs avoids a redundant check, because many of these contractors serve the FAA security program. The FAA also agrees that the responsibility for criminal history records checks of their contractors should be the responsibility of the airport operator.

FAA Response: This final rule adopts the procedures proposed in the SNPRM for accepting air carrier access investigations and non-air-carrier tenant employment history verifications. The rule does not attempt to establish uniform procedures for accepting transfers; rather, the rule sets the minimum requirement for continuous access to the FAA training. Under § 107.25 and associated FAA policy, individuals who have been subject to SIDA training who subsequently transfer their unescorted access must receive site-specific SIDA training at the new airport.

Individuals Subject To Investigation By Customs

One commenter suggests that the FAA coordinate with the U.S. Customs Service on its pending access rule for Customs Service security areas of an airport. The commenter’s concerns focus on the effect on operations, costs, and possible duplication of the two rules.

FAA Response: This rule permits an airport operator to accept the background checks performed by the U.S. Customs Service to meet the FAA’s access investigation requirement. Accepting the background investigation by Customs avoids a redundant check, because many of these contractors serve the FAA security program. The FAA also agrees that the responsibility for criminal history records checks of their contractors should be the responsibility of the airport operator.
the air carrier’s certification satisfies its regulatory obligation. The airport operator may accept a written statement that the employment history verification and, where appropriate, the criminal history records check were performed as part of the process of an air carrier issuing identification credentials to its employees. If a specific air carrier employee or its contractor employee is receiving airport-issued identification, the airport operator must receive certification for each employee prior to issuing an identification credential. The certification should include a statement that the investigation was conducted in accordance with §108.33 and provide the name(s) of the individual(s) requiring the unescorted access authority credential. However, the air carrier must retain the specific documentation supporting the access investigation.

The rule also includes a provision permitting an airport operator to accept written certification from airport tenants that they have reviewed the applicant’s 10-year employment history and verified the most recent 5 years of that history. Again, the airport tenant should retain the specific documentation supporting this certification. Pursuant to the Act, only airport operators and air carriers can request a criminal history records check, although the costs of such checks will normally be borne by the employer. Thus, the airport operator must process criminal history records checks for all airport tenants other than U.S. air carriers. However, the airport operator is responsible only for the unescorted access privilege determination. Employment-related decisions such as hiring and firing, and an individual’s status while a criminal history records check is pending, rest with the airport tenant.

For purposes of this rule, non-air-carrier tenants include airline food service companies, fixed base operators, foreign air carriers, and indirect air carriers subject to part 109 whose employees receive airport identification.

Section 107.31(g)—Appointing Contact

Six commenters respond to the issue of the airport operator appointing a person who will be responsible for reviewing the results of the employment investigation, determining an individual’s eligibility for unescorted access and serving as the liaison if the individual disputes the results of a criminal check. As proposed in the SNPRM, the appointed person could delegate the day-to-day duties, but would be the airport operator’s point of contact with the airport for purposes of monitoring compliance with the employment investigation requirement. In the SNPRM, the FAA also solicited comments on whether it should require the contact to be the airport security coordinator (ASC). Five commenters acknowledged that the ASC would be the contact, but believe the FAA should not require or specify the position.

FAA Response: This final rule requires the airport operator to designate the ASC required under §107.29 as the contact for access investigations. The ASC can delegate the duties while continuing to serve as the FAA’s point of contact with the airport for purposes of monitoring compliance with this rule. This is consistent with the requirements of §107.29 that the ASC serve as the airport operator’s primary contact for security-related activities and communications with the FAA.

The ASC, or designee, is responsible for reviewing the results of the access investigation and determining an individual’s eligibility for unescorted access privileges. The ASC also serves as the liaison when the individual disputes the results of the criminal history records check that revealed information that would disqualify the person from unescorted access.

Section 107.31(h)—Individual Notification

The FAA received no comments on this section.

Note: An individual covered by this rule must be notified of the need for a criminal history records check prior to commencing the check. Because the FAA will serve as the entity to process the criminal history records check required by this rule, this section of the final rule is modified from that proposed in the SNPRM by removing the language related to designating an outside entity.

Section 107.31(i)—Fingerprint Processing

The Act provides the FAA Administrator, in consultation with the Attorney General, the authority to designate persons to obtain and transmit fingerprints, and receive the results of a criminal history records check. In the SNPRM, the FAA proposed allowing airport operators and air carriers to directly contact the FBI or use an outside entity to request and process the criminal history records checks. The Department of Justice has agreed that airport operators and air carriers may access the criminal records system. The FBI indicates concerns about the FAA’s SNPRM proposal to have multiple entities request the checks. The FBI recommends that the FAA serve as the central processor, suggesting the use of a system similar to that of the Nuclear Regulatory Commission (NRC). The NRC serves as the processor of FBI criminal history records checks for the nuclear industry.

Nine comments address the issue of having a centralized processor or “clearing house” batch and process the FBI criminal history records check requests. Many of the commenters note that the proposed language in the SNPRM would result in far fewer criminal history checks being conducted (compared to the NPRM) and question whether a non-governmental clearing house is feasible for so few requests. As an alternative, they recommend that the FAA serve as the processor.

Three commenters focus on the related issue of screening criminal history records check results. RAA supports the concept in the SNPRM that allows the airport operator and air carriers to review an individual’s complete record. Two commenters state that a complete FBI record should not be sent to the airport operator or air carrier; rather, the record should be screened in some manner to determine whether a disqualifying conviction occurred and only that information provided. These commenters believe there is a significant privacy issue involved in releasing an entire record.

The FAA has
requests submitted to the FAA by airport operators and air carriers. The FAA will serve as the clearinghouse in a manner similar to the NRC and will ensure fingerprint cards are forwarded to the FBI in a timely and cost effective manner. A $24.00 fee will enable the FAA to recover its cost of processing and obtaining the FBI records. The FAA will charge the same $24.00 user fee currently levied by FBI on the banking, securities, commodities futures trading industries and the NRC. The fee is subject to increase without prior notice upon determination by the FBI. Parties subject to this rule will be notified of fee increases by amendments to this rule in the future.

Upon completion of the FBI records check, the complete FBI record will be forwarded to the requesting entity. The regulation places specific limits on the use of the information contained in the criminal history records check. This issue is addresed in the preamble discussion of § 107.31(m).

This final rule incorporates the possibility of using the NCIC system to allow airport operators and air carriers an alternative method for obtaining criminal history information for individuals applying for the privilege of unescorted access. As stated in the Notice of Public Meetings, and as discussed at the public meetings held on the initial notice, under published policy established by the NCIC's Advisory Policy Board, the NCIC is not available to check the records of applicants for employment in aviation related industries. In addition, checking an individual's name and other identifying information does not provide the same level of positive identification that derives from the use of a check based on an individual's fingerprints.

This final rule includes procedures for collecting fingerprints and requires that one set of legible fingerprints be taken on a card acceptable to the FBI (i.e., Federal Document 258). The airport operator may choose to have the airport law enforcement officers take the fingerprints. The FAA also requires verifying the individual's identity when taking his/her fingerprints. The individual must present two forms of identification, one of which must be the individual's photograph. A current driver's license, military identification, or passport are examples of acceptable photographic identification. In addition, the fingerprint cards must be handled and shipped in a manner that protects the privacy of the individual.

Airport operators will send the fingerprint cards to the Federal Aviation Administration, 800 Independence Ave. SW., Washington, DC 20591 (Attn: ACO–310. Access Processing). A corporate check, certified check, cashier's check or money order made payable to the "U.S. FA A" for $24.00 per card must accompany the request. The FAA will verify that the information required on the fingerprint cards is complete and forward the cards for processing. After the FBI completes the search of its index system, the FAA will receive the results and, in turn, will forward the results to the airport operator. Under this system, the airport operator will receive complete results of the check.

Section 107.31(j)—Making the Access Determination

Six commenters raise concerns over the airport operator or the air carrier being responsible for resolving any arrests for disqualifying crimes that have no disposition listed on the FBI criminal history records check result. ATA and RAA also suggest that the individual seeking employment should be responsible for furnishing any required disposition documentation.

FAA Response: This final rule requires the airport operator to ascertain the disposition of arrests for any of the enumerated offenses when no disposition has been recorded in the FBI's records, e.g., the case is pending or the FBI has no record. This task would be conducted with the affected individual and the jurisdiction where the arrest took place in order to determine whether a disposition has been recorded in that jurisdiction but not forwarded to the FBI. While the investigation will require assistance from the individual, it is the responsibility of the airport operator or the air carrier to complete the investigation. In determining whether to grant unescorted access an individual with an arrest for one of the disqualifying crimes with no disposition, the airport operator should weigh all relevant information available on the individual, including the results of the access investigation.

Section 107.31(k)—Availability and Correction of FBI Records and Notification of Disqualification

Two commenters state that allowing applicants to challenge the accuracy of the FBI record will require involvement by the airport operator in a possibly lengthy and expensive process.

FAA Response: The Act requires that individuals have the right to challenge the accuracy of their criminal history records. After the individual has a challenge may have a time consuming process, the FAA has no discretion to eliminate this right.

This rule does require the individual to notify the airport operator or its designee within 30 days of receipt of the record of his or her intent to correct any information believed to be inaccurate. Because the FBI maintains the records and has established procedures to address possible inaccuracies, it is appropriate to forward a copy of any requests for correction to the FBI. However, the FBI prefers that the actual request be made by the individual directly to the agency (i.e., federal, state or local jurisdiction) that supplied the questioned criminal history information to the FBI.

When taking the individual's fingerprints, the airport operator must notify the individual that he or she will be provided, upon written request, a copy of the results of the FBI criminal history records check prior to rendering the access decision.

If the airport operator is not notified by the individual within the 30-day period that he or she intends to dispute the results, the airport operator may make the final access decision. The airport operator is neither obligated to provide the individual with an escort before the correction (if any) is made, nor is the employer obligated to hire the applicant after the record is corrected. However, after being informed that the disqualifying information has been corrected, the airport operator would have to obtain a copy of the revised FBI record before the individual could be authorized for unescorted access.

If an individual is disqualified for unescorted access based on the findings of the criminal history record check, the individual must be notified that such a determination has been made.

Section 107.31(1)—Individual Accountability

Two commenters address the issue requiring an individual with unescorted access authority to report any disqualifying convictions occurring after the completion of the employment investigation. One commenter concurs with the decision not to require a recurrent investigation and another states that the SNPRM did not adequately address the procedures that would apply in these cases.

FAA Response: This final rule adopts the "self-disclosure" provision included in the SNPRM. Any person holding unescorted access authority who is convicted of any of the disqualifying crimes after January 31, 1995, must surrender the identification media to the FAA within 24 hours of learning of the conviction. This final rule does not provide additional guidance on this...
requirement. However, the FAA expects that the regulated parties will develop local procedures to implement this provision. In such cases, the employer is likely to be aware of the circumstances and take immediate action to revoke the access authority.

Any individual failing to report a disqualifying conviction or to surrender his or her SIDA identification credential issued under this section is subject to possible FAA enforcement action, including civil penalty liability.

Section 107.31(m)—Limits on Dissemination of Results

The FAA received no comments on this section.

**Note:** As required by the Act, this rule also includes limits on the dissemination of the criminal history information. The FAA limits distribution of such information to: (1) the individual to whom the record pertains or someone authorized by that person; (2) the airport operator; and (3) the individuals designated by the Administrator, e.g., FAA special agents.

Section 107.31(n)—Recordkeeping

Six commenters address the requirements for maintaining records. ATA requests that the final rule clearly require maintaining only that information necessary to satisfy the regulation requirements. The FAA has modified this section.

**FAA Response:** The FAA has determined that the final rule clearly requires maintaining only that information necessary to satisfy the regulation requirements. ATA is concerned that FAA inspectors may interpret the record provision as providing discretion to require the maintenance of information beyond that which is necessary to meet the requirements set forth in the SNPRM.

Two airport operators express concerns over the administrative burden of maintaining all employment history records of non-air-carrier tenants. One commenter agrees that maintaining the criminal history records checks is the airport operator’s responsibility and that this should not be a burden to airports because they already keep confidential information.

**FAA Response:** The FAA has determined that the airport or air carrier shall maintain a written record for individuals granted unescorted access that includes specific information on the employment history verification and the results of an FBI criminal history records check, if conducted. The burden on airport operators to maintain records for tenants already exists because airport operators maintain records for individuals who are currently issued identification media. This rule standardizes the information to be maintained to include the results of the FBI criminal history records check, where applicable. The airport tenant can continue to maintain the more comprehensive record and associated paperwork of the employment history verification.

The FAA has modified this section from that proposed in the SNPRM to clarify that an airport operator need not maintain comprehensive records and documentation for air carrier employees. As discussed under §107.31(f), the record can be a certification from the air carrier that the access investigation was performed. The air carrier operator would have no further recordkeeping requirements related to air carrier employees. Furthermore, in order to permit the destruction of FBI criminal history records check results and minimize storage problems for airport operators and air carriers, the recordkeeping requirements allow for the retention of only a certification that the check was completed and revealed no disqualifying convictions. Another minor editorial change in this regard was the deletion of the reference to airport tenants providing certification of criminal history records check results since these parties are not authorized to request such checks.

This final rule contains two recordkeeping requirements: (1) A record indicating that the applicant’s 10-year employment history has been reviewed and the most recent 5-year employment history verified, and (2) a copy of the results of the criminal history record check received from the FBI or certification of same, where appropriate. The airport operator can accept written certification from airport tenants that the employment history was reviewed and the verification was performed. However, the airport tenant should maintain a record of calls made, plus a record of correspondence or any other documents received. The tenant must make this information available to the airport operator when requested by the FAA for inspection purposes.

For individuals subject to a criminal history records check, the records received from the FBI must be maintained in a manner that prevents the unauthorized dissemination of its contents.

The airport operator must maintain a written record until 180 days after termination of the individual’s authority.

Section 108.33—Employment Verification

This rule authorizes air carriers to perform the access investigations for its employees and contractors in a manner similar to that required under §107.31. The air carrier may provide a general certification to an airport operator under §107.31(f) that the access investigation was performed as part of issuing identification credentials to its employees. When an individual air carrier employee or its contractor employee is investigated by the carrier for receipt of airport-issued identification media, the air carrier must provide the airport operator with certification that the investigation was performed for each employee.

The requirements for an air carrier performing the access investigation are identical to those required of an airport operator.

**Regulatory Evaluation Summary**

Changes to Federal regulations are required to undergo several economic analyses. First, Executive Order 12866 directs each Federal agency to propose or adopt a regulation only upon a reasoned determination that the benefits of the intended regulation justify its costs. Second, the Regulatory Flexibility Act of 1980 requires agencies to analyze the economic effects of regulatory changes on small entities. Third, the Office of Management and Budget directs agencies to assess the effect of regulatory changes on international trade. With respect to this rule, the FAA has determined that it: (1) is “a significant regulatory action” as defined in section 3(f)(4) of the Executive Order; (2) is significant as defined in the Department of Transportation’s Regulatory Policies and Procedures; (3) will not have a significant impact on a substantial number of small entities; and (4) will not constitute a barrier to international trade. Since the rule is not significant under section 3(f)(4) of the Executive Order, a full regulatory analysis, which includes the identification and evaluation of cost-reducing alternatives to this rule, has not been prepared. Instead, the agency has prepared a more concise analysis of this rule which is presented in the following paragraphs.

The expected costs of the rule consist of two parts: (1) the cost of enhancing the employment history verification process; and (2) the cost of conducting a criminal history records check on applicants whose employment verification triggers it. Employers may avoid the latter cost by simply choosing to end the employment process for the individual in question.

First-year costs for the industry will range from $0.5 to $1.4 million. Airports, air carriers, and other airport tenants will incur these costs. The cost of the rule comes from the unique cost necessary to complete the required 64,000 criminal history verifications by non-air-carrier airport tenants and from an estimated 970 to 1,940 criminal
history records checks by all airport and air carrier employers. The FAA estimates that, in 1995, 194,000 employees will apply for unescorted SIDA access privilege. Between 1995 and 2004, the total cost of the new requirements will range from $6.2 to $16.2 million. The discounted cost ranges from $4.3 to $11.1 million.

Because aviation security requires an intricate set of interlocking measures, the benefits ascribed to this final rule derive from strengthening the U.S. civil aviation security network. By enhancing the civil aviation security network, this final rule decreases the possibility that a deadly and costly terrorist or criminal act will occur. This final rule assures a greater measure of safety through tighter screening of individuals applying for jobs requiring unescorted secure area access. Specifically, this final rule reduces the civil aviation security risk by further assuring that persons who have committed certain crimes do not have access to airport secure areas. The FAA determined that the final rule provides sufficient additional security to make it cost beneficial.

The rule will have a negligible impact on international trade. Also, the proposed regulatory action will not have a significant economic impact on a substantial number of small entities.

Final Regulatory Flexibility Determination

The Regulatory Flexibility Act of 1980 (RFA) helps to assure that Federal regulations do not overly burden small businesses, nonprofit organizations, and small cities. The RFA requires regulatory agencies to review rules which may have “a significant economic impact on a substantial number of small entities.” A substantial number of small entities, defined by FAA Order 2100.14A—“Regulatory Flexibility Criteria and Guidance,” is more than one-third, but not less than eleven, of the small entities subject to the existing rule. To determine if the rule will impose a significant cost impact on these small entities, the annualized cost imposed on them must not exceed the annualized cost threshold established in FAA Order 2100.14A.

Small entities potentially affected by the rule are small airports, air carriers, fixed-base operators, and catering companies. However, many of the requirements of the rule are already standard procedures for some of these entities; and the cost of a criminal history records check is minimal because small employers are expected to use it for their applicants. The FAA estimates the average cost of upgrading an employee verification is $15.00. This estimate incorporates the cost of a criminal history records checks.

Aircraft Repair Facilities: FAA Order 2100.14A defines small aircraft repair facilities as those with 200 employees or less. The FAA has estimated the cost threshold for small operators to be $4,130 in 1992 dollars. To exceed this threshold, a facility would have to hire 275 employees ($4,130/$15.00) per year. This means that the facility would have to regularly employ 786 persons (assuming a 35 percent turnover rate: 275/35). If a firm employed that many people, it would be a small entity since it is over the size threshold of 200 employees.

Caterers: The FAA evaluates small caterers as aircraft repair facilities since FAA Order 2100.14A does not define a threshold for caterers. This order defines the criteria as 200 employees or less for the size threshold and $4,130 for the cost threshold. Hence, like the aircraft repair facilities, in order to exceed the cost threshold, caterers would have to employ 786 persons, which would exceed the size threshold of 200 employees.

In conclusion, the rule will not impose a significant impact on a substantial number of small entities.

Federalism Implications

This rule does not have a substantial direct effect on the states, on the relationship between the national government and the states, or on the distribution of power and responsibilities among the various levels of government. Most airports covered by the rule are public entities (state and local governments). However, relatively few of the covered individuals are actually employed by the airport operator, and most of the costs for the required investigations would be borne by the airport tenants and air carriers. Thus, the overall impact is not substantial within the meaning of Executive Order 12612. Therefore, in accordance with that Executive Order, it is determined that this rule would not have sufficient Federal implications to warrant the preparation of a Federalism Assessment.

International Civil Aviation Organization and Joint Aviation Regulations

In keeping with U.S. obligations under the Convention on International Civil Aviation, it is FAA policy to comply with International Civil Aviation Organization Standards and Recommended Practices to the maximum extent practicable. The FAA is not aware of any differences that this final rule will present.

Paperwork Reduction Act

Under the requirements of the Federal Paperwork Reduction Act, the Office of Management and Budget has approved the information collection burden for this rule under OMB Approval Number 2120–0564. For further information contact: The Information Requirements Division, M–34, Office of the Secretary of Transportation, 400 Seventh Street, SW., Washington, D.C., 20590, (202) 366–4375 or Edward Clarke or Wayne Brough, Office of Management and Budget, New Executive Office Building, Room 3228, Washington D.C., 20503, (202) 395–7340.

Conclusion

For the reasons discussed in the preamble, and based on the findings in the Regulatory Flexibility Determination and the International Trade Impact Analysis, the FAA has determined that this rule is a significant regulatory action under Executive Order 12866. This rule will not have a significant economic impact on a substantial number of small entities under the criteria of the Regulatory Flexibility Act but is considered significant under DOT Regulatory Policies and Procedures (44 FR 11034; February 26, 1979). The regulatory evaluation for this rule, including a Regulatory Flexibility Determination and International Trade Impact Analysis, has been placed in the docket. A copy may be obtained by contacting the person identified under FOR FURTHER INFORMATION CONTACT.

List of Subjects in 14 CFR Parts 107 and 108

Air carriers, Air Transportation, Airlines, Airplanes operator security, Aviation safety, Security measures, Transportation, Weapons.

The Rule Amendments

In consideration of the foregoing, the Federal Aviation Administration amends parts 107 and 108 of the Federal Aviation Regulations (14 CFR parts 107 and 108) as follows:

PART 107—AIRPORT SECURITY

1. The authority citation for Part 107 is revised to read as follows:


2. In part 107, § 107.1 paragraphs (b)(3) through (b)(5) are redesignated as paragraphs (b)(4) through (b)(6), and...
new paragraph (b)(3) is added to read as follows:

§ 107.1  Applicability and Definitions.

(b) * * * *

(3) Escort means to accompany or supervise an individual who does not have unescorted access authority to areas restricted for security purposes, as identified in the airport security program, in a manner sufficient to take action to prevent the individual from engaging in activities other than those for which the escorted access is granted. The responsive actions can be taken by the escort or other authorized individual. * * * *

3. Part 107 is amended by adding a new § 107.31 to read as follows:

§ 107.31  Access Investigation

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

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

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

(2) The results of the access investigation do not disclose that the individual has been convicted or found not guilty by reason of insanity, in any jurisdiction, during the 10 years ending on the date of such investigation, of any of the following crimes:

(i) The individual's full name, including any aliases or nicknames;
(ii) The dates, names, phone numbers, and addresses of previous employers, with explanations for any gaps in employment of more than 12 months, during the previous 10-year period;
(iii) Notification that the individual will be subject to an employment history verification and possibly a criminal history records check; and
(iv) Any convictions during the previous 10-year period of the crimes listed in paragraph (b)(2) of this section.

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

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

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

(i) The individual cannot satisfactorily account for a period of unemployment of 12 months or more during the previous 10-year period;
(ii) The individual is unable to support statements made or there are significant inconsistencies between information provided on the application in response to questions required by paragraph (c)(1)(ii) of this section and that obtained through the 5-year verification process; or
(iii) Information becomes available to the airport operator during the access investigation indicating a possible conviction for one of the disqualifying crimes.

(d) An airport operator may permit an individual to be under escort as defined in § 107.1 in accordance with this section in an area identified in paragraph (a) of this section.

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

(1) Employees of the Federal government or a state or local government (including law enforcement officers) who, as a condition of employment, have been subject to an employment investigation;
(2) Crew members of foreign air carriers covered by an alternate security arrangement in the approved airport operator security program;
(3) An individual who has been continuously employed in a position requiring unescorted access by another airport operator, airport tenant or air carrier; and
(4) An individual who has access authority to the U.S. Customs Service security area of the U.S. airport.

(f) An airport operator will be deemed to be in compliance with its obligations under paragraphs (b)(1) and (b)(2) of this section, as applicable, when it accepts certification from:
(1) An air carrier subject to §108.33 of this chapter that the air carrier has complied with §108.33 (a)(1) and (a)(2) for its employees and contractors; and
(2) An airport tenant other than a U.S. air carrier that the tenant has complied with paragraph (b)(1) of this section for its employees.

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

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

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

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

(1) One set of legible and classifiable fingerprints must be recorded on fingerprint cards approved by the FBI for this purpose;
(2) The fingerprints must be obtained from the individual under direct observation by the airport operator;
(3) The identity of the individual must be verified at the time fingerprints are obtained. The individual must present two forms of identification media, one of which must bear his or her photograph;
(4) The fingerprint card must be forwarded to Federal Aviation Administration, 800 Independence Ave., S.W., Washington, D.C. 20591 (ATTN: ACO–310, Access Processing); and
(5) Fees for the processing of the criminal checks are due upon application. Airport operators shall submit payment through corporate check, cashier's check or money order made payable to “U.S. FAA,” at the rate of $24.00 for each fingerprint card. Combined payment for multiple applications is acceptable.

(j) In conducting the criminal history records check required by this section, the airport operator must ascertain information on arrests for the crimes listed in paragraph (b)(2) of this section for which no disposition has been recorded to make a determination of the individual's authority for unescorted access. These records must be maintained in a manner that protects the confidentiality of the employee, which is acceptable to the Assistant Administrator for Civil Aviation Security.

PART 108—AIRPLANE OPERATOR SECURITY

4. The authority citation for Part 108 is revised to read as follows:


5. Part 108 is amended by adding a new §108.33 to read as follows:

§108.33 Access investigation.

(a) On or after January 31, 1996 for each employee or contractor employee covered under a certification made to an airport operator pursuant to §107.31(f) of this chapter, the certificate holder must ensure that:

(1) The individual has satisfactorily undergone an employment history review covering the past 10 years and verification of the 5 years preceding the date the access investigation is initiated as provided in paragraph (b) of this section; and
(2) The results of the access investigation do not disclose that the individual has been convicted or found not guilty by reason of insanity, in any jurisdiction, during the 10 years ending on the date of such investigation, of any of the following crimes enumerated in paragraphs (i) through (xxv) of this section. Where specific citations are listed, both the current citation and the citation that applied before the statutes are recodified in 1994 are listed.

(i) Forgery of certificates, false marking of aircraft, and other aircraft registration violation, 49 U.S.C. 46306 [formerly 49 U.S.C. App. 1472(b)];
(ii) Interference with flightcrew members or flight attendants, 49 U.S.C. 46304 [formerly 49 U.S.C. App. 1472(c)];
(iii) Improper transportation of a hazardous material, 49 U.S.C. 46312, [formerly 49 U.S.C. App. 1472(b)(2)];
(v) Interference with flightcrew members or flight attendants, 49 U.S.C. 46304 [formerly 49 U.S.C. App. 1472(c)];
(vi) Commission of certain crimes aboard aircraft in flight, 49 U.S.C.
(vi) Carrying or using a weapon of mass destruction, 18 U.S.C. 32; or

(vii) Carrying or using an explosive, 18 U.S.C. 3056.

(b) The access investigation must indicate a possible disqualifying criminal history. A final access decision cannot include such a history record if the certificate holder does not make a final decision to grant or deny access.

(c) The certificate holder must designate an individual to review and control the criminal history record received from the FBI prior to making a final access decision.

(d) Prior to making a final access decision, the certificate holder must make a final decision to grant or deny access.

(e) The certificate holder must retain a copy of the criminal history record received from the FBI for 30 days after the final access decision.

(f) The certificate holder must notify the individual that the criminal history record is available to any final access decision.

(g) The certificate holder must notify the individual that the criminal history record is available to any final access decision.

(h) The certificate holder must notify the individual that the criminal history record is available to any final access decision.

(i) The certificate holder must notify the individual that the criminal history record is available to any final access decision.

(j) The certificate holder must notify the individual that the criminal history record is available to any final access decision.

(k) The certificate holder must notify the individual that the criminal history record is available to any final access decision.

(l) The certificate holder must notify the individual that the criminal history record is available to any final access decision.

(m) The certificate holder must notify the individual that the criminal history record is available to any final access decision.

(n) The certificate holder must notify the individual that the criminal history record is available to any final access decision.

(o) The certificate holder must notify the individual that the criminal history record is available to any final access decision.

(p) The certificate holder must notify the individual that the criminal history record is available to any final access decision.

(q) The certificate holder must notify the individual that the criminal history record is available to any final access decision.

(r) The certificate holder must notify the individual that the criminal history record is available to any final access decision.

(s) The certificate holder must notify the individual that the criminal history record is available to any final access decision.

(t) The certificate holder must notify the individual that the criminal history record is available to any final access decision.

(u) The certificate holder must notify the individual that the criminal history record is available to any final access decision.

(v) The certificate holder must notify the individual that the criminal history record is available to any final access decision.

(w) The certificate holder must notify the individual that the criminal history record is available to any final access decision.

(x) The certificate holder must notify the individual that the criminal history record is available to any final access decision.

(y) The certificate holder must notify the individual that the criminal history record is available to any final access decision.

(z) The certificate holder must notify the individual that the criminal history record is available to any final access decision.

(1) The certificate holder must notify the individual that the criminal history record is available to any final access decision.

(2) The certificate holder must notify the individual that the criminal history record is available to any final access decision.

(3) The certificate holder must notify the individual that the criminal history record is available to any final access decision.

(4) The certificate holder must notify the individual that the criminal history record is available to any final access decision.

(5) The certificate holder must notify the individual that the criminal history record is available to any final access decision.

(6) The certificate holder must notify the individual that the criminal history record is available to any final access decision.

(7) The certificate holder must notify the individual that the criminal history record is available to any final access decision.

(8) The certificate holder must notify the individual that the criminal history record is available to any final access decision.

(9) The certificate holder must notify the individual that the criminal history record is available to any final access decision.

(10) The certificate holder must notify the individual that the criminal history record is available to any final access decision.

(11) The certificate holder must notify the individual that the criminal history record is available to any final access decision.

(12) The certificate holder must notify the individual that the criminal history record is available to any final access decision.

(13) The certificate holder must notify the individual that the criminal history record is available to any final access decision.

(14) The certificate holder must notify the individual that the criminal history record is available to any final access decision.

(15) The certificate holder must notify the individual that the criminal history record is available to any final access decision.

(16) The certificate holder must notify the individual that the criminal history record is available to any final access decision.

(17) The certificate holder must notify the individual that the criminal history record is available to any final access decision.

(18) The certificate holder must notify the individual that the criminal history record is available to any final access decision.

(19) The certificate holder must notify the individual that the criminal history record is available to any final access decision.

(20) The certificate holder must notify the individual that the criminal history record is available to any final access decision.

(21) The certificate holder must notify the individual that the criminal history record is available to any final access decision.

(22) The certificate holder must notify the individual that the criminal history record is available to any final access decision.

(23) The certificate holder must notify the individual that the criminal history record is available to any final access decision.

(24) The certificate holder must notify the individual that the criminal history record is available to any final access decision.

(25) The certificate holder must notify the individual that the criminal history record is available to any final access decision.

(26) The certificate holder must notify the individual that the criminal history record is available to any final access decision.

(27) The certificate holder must notify the individual that the criminal history record is available to any final access decision.

(28) The certificate holder must notify the individual that the criminal history record is available to any final access decision.

(29) The certificate holder must notify the individual that the criminal history record is available to any final access decision.

(30) The certificate holder must notify the individual that the criminal history record is available to any final access decision.

(31) The certificate holder must notify the individual that the criminal history record is available to any final access decision.

(32) The certificate holder must notify the individual that the criminal history record is available to any final access decision.

(33) The certificate holder must notify the individual that the criminal history record is available to any final access decision.

(34) The certificate holder must notify the individual that the criminal history record is available to any final access decision.

(35) The certificate holder must notify the individual that the criminal history record is available to any final access decision.

(36) The certificate holder must notify the individual that the criminal history record is available to any final access decision.

(37) The certificate holder must notify the individual that the criminal history record is available to any final access decision.

(38) The certificate holder must notify the individual that the criminal history record is available to any final access decision.

(39) The certificate holder must notify the individual that the criminal history record is available to any final access decision.

(40) The certificate holder must notify the individual that the criminal history record is available to any final access decision.

(41) The certificate holder must notify the individual that the criminal history record is available to any final access decision.

(42) The certificate holder must notify the individual that the criminal history record is available to any final access decision.

(43) The certificate holder must notify the individual that the criminal history record is available to any final access decision.

(44) The certificate holder must notify the individual that the criminal history record is available to any final access decision.

(45) The certificate holder must notify the individual that the criminal history record is available to any final access decision.

(46) The certificate holder must notify the individual that the criminal history record is available to any final access decision.

(47) The certificate holder must notify the individual that the criminal history record is available to any final access decision.

(48) The certificate holder must notify the individual that the criminal history record is available to any final access decision.

(49) The certificate holder must notify the individual that the criminal history record is available to any final access decision.

(50) The certificate holder must notify the individual that the criminal history record is available to any final access decision.

(51) The certificate holder must notify the individual that the criminal history record is available to any final access decision.

(52) The certificate holder must notify the individual that the criminal history record is available to any final access decision.

(53) The certificate holder must notify the individual that the criminal history record is available to any final access decision.

(54) The certificate holder must notify the individual that the criminal history record is available to any final access decision.

(55) The certificate holder must notify the individual that the criminal history record is available to any final access decision.

(56) The certificate holder must notify the individual that the criminal history record is available to any final access decision.

(57) The certificate holder must notify the individual that the criminal history record is available to any final access decision.

(58) The certificate holder must notify the individual that the criminal history record is available to any final access decision.

(59) The certificate holder must notify the individual that the criminal history record is available to any final access decision.

(60) The certificate holder must notify the individual that the criminal history record is available to any final access decision.

(61) The certificate holder must notify the individual that the criminal history record is available to any final access decision.

(62) The certificate holder must notify the individual that the criminal history record is available to any final access decision.

(63) The certificate holder must notify the individual that the criminal history record is available to any final access decision.

(64) The certificate holder must notify the individual that the criminal history record is available to any final access decision.

(65) The certificate holder must notify the individual that the criminal history record is available to any final access decision.

(66) The certificate holder must notify the individual that the criminal history record is available to any final access decision.

(67) The certificate holder must notify the individual that the criminal history record is available to any final access decision.

(68) The certificate holder must notify the individual that the criminal history record is available to any final access decision.

(69) The certificate holder must notify the individual that the criminal history record is available to any final access decision.

(70) The certificate holder must notify the individual that the criminal history record is available to any final access decision.

(71) The certificate holder must notify the individual that the criminal history record is available to any final access decision.

(72) The certificate holder must notify the individual that the criminal history record is available to any final access decision.

(73) The certificate holder must notify the individual that the criminal history record is available to any final access decision.

(74) The certificate holder must notify the individual that the criminal history record is available to any final access decision.

(75) The certificate holder must notify the individual that the criminal history record is available to any final access decision.

(76) The certificate holder must notify the individual that the criminal history record is available to any final access decision.

(77) The certificate holder must notify the individual that the criminal history record is available to any final access decision.

(78) The certificate holder must notify the individual that the criminal history record is available to any final access decision.

(79) The certificate holder must notify the individual that the criminal history record is available to any final access decision.

(80) The certificate holder must notify the individual that the criminal history record is available to any final access decision.

(81) The certificate holder must notify the individual that the criminal history record is available to any final access decision.

(82) The certificate holder must notify the individual that the criminal history record is available to any final access decision.

(83) The certificate holder must notify the individual that the criminal history record is available to any final access decision. 
(1) The individual to whom the record pertains or that individual’s authorized representative;

(2) The certificate holder; or

(3) Others designated by the Administrator.

(j) The certificate holder must maintain a written record that the investigation was conducted for the individual until 180 days after the termination of the individual’s authority for unescorted access. The record for individuals subject to:

(1) The access investigation must include the application, the employment verification information obtained by the employer, the names of those from whom the employment verification information was obtained, the date the contact was made, and any other information as required by the Assistant Administrator for Civil Aviation Security, and

(2) A criminal history records check must include the results of the records check or certification by the air carrier that a check was completed and did not uncover a disqualifying conviction. These records must be maintained in a manner that protects the confidentiality of the employee, which is acceptable to the Assistant Administrator for Civil Aviation Security.

Issued in Washington, DC, on September 26, 1995.

David R. Hinson,
Administrator.

[FR Doc. 95–24546 Filed 9–28–95; 3:10 pm]
BILLING CODE 4910–13–M
Corrections

This section of the FEDERAL REGISTER contains editorial corrections of previously published Presidential, Rule, Proposed Rule, and Notice documents. These corrections are prepared by the Office of the Federal Register. Agency prepared corrections are issued as signed documents and appear in the appropriate document categories elsewhere in the issue.

DEPARTMENT OF TRANSPORTATION

Federal Aviation Administration

14 CFR Parts 107 and 108

[Docket No. 26763; Amendment Nos. 107-7, 108-12]

RIN2120-AE14

Unescorted Access Privilege

Correction

In rule document 95–24546 beginning on page 51854 in the issue of Tuesday, October 3, 1995 make the following corrections:

1. On page 51861, middle column, fourteenth line, “suggest” should read “suggests”.

2. On page 51865, third column, last paragraph, sixth line, “1995” should read “1996”.

BILLING CODE 1505-01-D
Department of Transportation

Federal Aviation Administration

14 CFR Parts 107 and 108
Unescorted Access Privilege: Address Change; Final Rule
Persons interested in being placed on the mailing list for future Notices of Proposed Rulemaking and Final Rules should request from the above office a copy of Advisory Circular No. 11-2A, Notice of Proposed Rulemaking Distribution System, that describes the application procedure.

Background

Amendments 107-7 and 108-12 required airport operators and air carriers to conduct employment investigations and disqualify individuals convicted of certain enumerated crimes from having, or being able to authorize others to have, unescorted access privileges to a security identification display area (SIDA) of a U.S. airport. (60 FR 51854; October 3, 1995.) This rulemaking was promulgated to enhance the effectiveness of the U.S. civil aviation security system by ensuring that individuals applying for unescorted access privileges do not constitute an unreasonable risk to the security of the aviation system.

One of the requirements of the final rule is that airport operators, under part 107, and air carriers, under part 108, submit the fingerprint cards required for certain employment investigation checks to the FAA at its 800 Independence Ave., NW., Washington, DC address. However, for administrative reasons, the Office of Civil Aviation Security has determined that the cards could be more efficiently processed at the FAA field office in St. Louis, Missouri. Therefore, the FAA is amending the rules to indicate this change of address. The newly designated office to receive the fingerprint cards is: Federal Aviation Administration, Room 4597E, 9700 Page Avenue, St. Louis, MO 63132.

Readers will observe that this address does not appear in the amended regulatory language. The reason for not putting a specific address in the rule language is that, for every change to this address, the FAA must amend the regulations, a process that expends resources unnecessarily. However, the FAA also realizes that, in the future, if a change in address occurs, airport operators and air carriers must, as a practical matter, have such information quickly. Therefore, the FAA had determined that it will disclose any changes via the respective security programs to ensure that airport operators and air carriers are notified of any change of address in an expeditious manner.

This change of address is effective in 30 days. The FAA believes that this constitutes sufficient notice for affected persons to effect the change.

Regulatory Process Matters

Because this is an administrative change with no substantive effect on any regulation and because the change of address constitutes no costs to regulated parties, the FAA has determined that prior notice and comment is unnecessary. The FAA also certifies that this administrative change will not impose a significant impact on small entities. In addition, it has also been determined that this final rule change is not a “significant regulatory action” under Executive Order 12866 nor is it a significant action under DOT regulatory policies and procedures (44 FR 11034, February 26, 1979).

Paperwork Reduction Act

Information collection requirements found in § 107.31 and 108.33 have been approved by the Office of Management and Budget (OMB) under the provisions of the Paperwork Reduction Act of 1995 (44 U.S.C. 3507(d)), and have been assigned OMB Control Number 2120-0564. There are no new requirements for information collection associated with this amendment.

List of Subjects in 14 CFR Parts 107 and 108

Air carriers, Air transportation, Airlines, Airplanes operator security, Aviation safety, Security matters, Transportation, Weapons.

The Amendment

In consideration of the foregoing, the Federal Aviation Administration amends parts 107 and 108 of Title 14, Code of Federal Regulations as follows:

PART 107—AIRPORT SECURITY

1. The authority citation for part 107 continues to read as follows:


2. Amend § 107.31 to revise paragraph (i)(4) to read as follows:

§ 107.31 Access investigation.

(i) * * * * *

(4) The fingerprint card must be forwarded to the Federal Aviation Administration at the location specified by the Administrator.

* * * * *

DEPARTMENT OF TRANSPORTATION

Federal Aviation Administration

14 CFR Parts 107 and 108

[Docket No. 29193; Amendment No. 107–11; 108–16]

Unescorted Access Privileges: Address Change

AGENCY: Federal Aviation Administration (FAA), DOT.

ACTION: Final rule.

SUMMARY: In October 1995, the FAA published a final rule requiring employment history checks for individuals authorized access to a security identification display area (SIDA) of a U.S. airport. This final rule changes the Federal Aviation Administration address to which fingerprint cards required for certain employment checks must be forwarded. This final rule announces an administrative decision internal to the FAA and does not affect the substance of the October 1995 final rule.


SUPPLEMENTARY INFORMATION

Availability of Final Rules

An electronic copy of this document may be downloaded using a modem and suitable communications software from the FAA regulations section of the Fedworld electronic bulletin board service (telephone: 703–321–3339), the Federal Register's electronic bulletin board service (telephone: 202–512–1661), or the FAA's Aviation Rulemaking Advisory Committee Bulletin Board service (telephone: 800–FAA–ARAC).

Internet users may reach the FAA's web page at http://www.faa.gov or the Federal Register's webpage at http://www.access.gpo.gov/su_docs for access to recently published rulemaking documents.

Any person may obtain a copy of this final rule by submitting a request to the Federal Aviation Administration, Office of Rulemaking, ARM–1, 800 Independence Avenue, SW., Washington, DC 20591, or by calling (202) 267–9680. Communications must identify the amendment number or docket number of this final rule.

Persons interested in being placed on the mailing list for future Notices of Proposed Rulemaking and Final Rules should request from the above office a copy of Advisory Circular No. 11-2A, Notice of Proposed Rulemaking Distribution System, that describes the application procedure.

Background

Amendments 107–7 and 108–12 required airport operators and air carriers to conduct employment investigations and disqualify individuals convicted of certain enumerated crimes from having, or being able to authorize others to have, unescorted access privileges to a security identification display area (SIDA) of a U.S. airport. (60 FR 51854; October 3, 1995.) This rulemaking was promulgated to enhance the effectiveness of the U.S. civil aviation security system by ensuring that individuals applying for unescorted access privileges do not constitute an unreasonable risk to the security of the aviation system.

One of the requirements of the final rule is that airport operators, under part 107, and air carriers, under part 108, submit the fingerprint cards required for certain employment investigation checks to the FAA at its 800 Independence Ave., NW., Washington, DC address. However, for administrative reasons, the Office of Civil Aviation Security has determined that the cards could be more efficiently processed at the FAA field office in St. Louis, Missouri. Therefore, the FAA is amending the rules to indicate this change of address. The newly designated office to receive the fingerprint cards is: Federal Aviation Administration, Room 4597E, 9700 Page Avenue, St. Louis, MO 63132.

Readers will observe that this address does not appear in the amended regulatory language. The reason for not putting a specific address in the rule language is that, for every change to this address, the FAA must amend the regulations, a process that expends resources unnecessarily. However, the FAA also realizes that, in the future, if a change in address occurs, airport operators and air carriers must, as a practical matter, have such information quickly. Therefore, the FAA had determined that it will disclose any changes via the respective security programs to ensure that airport operators and air carriers are notified of any change of address in an expeditious manner.

This change of address is effective in 30 days. The FAA believes that this constitutes sufficient notice for affected persons to effect the change.

Regulatory Process Matters

Because this is an administrative change with no substantive effect on any regulation and because the change of address constitutes no costs to regulated parties, the FAA has determined that prior notice and comment is unnecessary. The FAA also certifies that this administrative change will not impose a significant impact on small entities. In addition, it has also been determined that this final rule change is not a “significant regulatory action” under Executive Order 12866 nor is it a significant action under DOT regulatory policies and procedures (44 FR 11034, February 26, 1979).

Paperwork Reduction Act

Information collection requirements found in § 107.31 and 108.33 have been approved by the Office of Management and Budget (OMB) under the provisions of the Paperwork Reduction Act of 1995 (44 U.S.C. 3507(d)), and have been assigned OMB Control Number 2120–0564. There are no new requirements for information collection associated with this amendment.

List of Subjects in 14 CFR Parts 107 and 108

Air carriers, Air transportation, Airlines, Airplanes operator security, Aviation safety, Security matters, Transportation, Weapons.

The Amendment

In consideration of the foregoing, the Federal Aviation Administration amends parts 107 and 108 of Title 14, Code of Federal Regulations as follows:

PART 107—AIRPORT SECURITY

1. The authority citation for part 107 continues to read as follows:


2. Amend § 107.31 to revise paragraph (i)(4) to read as follows:

§ 107.31 Access investigation.

(i) * * * * *

(4) The fingerprint card must be forwarded to the Federal Aviation Administration at the location specified by the Administrator.

* * * * *
PART 108—AIRPLANE OPERATOR SECURITY

3. The authority citation for part 108 continues to read as follows:


4. Amend § 108.33 to revise paragraph (e)(4) to read as follows:

§ 108.33 Access investigation.

  (e) * * * * *

  (4) The fingerprint card must be forwarded to the Federal Aviation Administration at the location specified by the Administrator.

* * * * *

Issued in Washington, DC on April 7, 1998.

Jane F. Garvey,
Administrator.

[FR Doc. 98–9643 Filed 4–10–98; 8:45 am]

BILLING CODE 4910–13–M