

**U.S. DEPARTMENT OF
HOMELAND SECURITY**

Transportation Security
Administration

Aviation Security Directive

Subject: Security Threat Assessment and Reporting Requirements Related to Individuals with Airport-Issued Identification Media

Number: SD 1542-04-08F

Date: December 10, 2008

EXPIRATION: Indefinite

This Security Directive (SD) cancels and supersedes **SD 1542-04-08E** and must be implemented immediately, except where otherwise noted. The measures contained in this SD are in addition to all other SDs currently in effect for your operations. **Changes to the previous SD are indicated in bold.**

INFORMATION: The threat to U.S. civil aviation remains significant. Current credible intelligence indicates Al-Qaida and other terrorist groups continue to develop plans for multiple attacks against targets in the United States, including airports and civil aviation. These terrorist groups continue to pursue a range of targets, tactics, and capabilities to accomplish this objective, including employment in the aviation sector to gain knowledge of aviation operations. Terrorist operatives view attacks on the United States as a priority because of their potentially significant economic and psychological impacts.

The Transportation Security Administration (TSA) has determined that to maintain effective security at the airport, there is a need to revise the requirements regarding issuance of airport-issued identification media and the individuals who apply for or hold identification media at the airport. This information includes **improved identification verification and work authorization status**, which TSA needs to perform a thorough Security Threat Assessment (STA). This SD responds to the continuing threat by modifying and improving TSA's ability to monitor the status of individuals who hold or apply for any type of identification media issued by the airport operator and prohibiting the issuance of any airport identification media until the information requested by TSA is received and TSA has completed an STA.

REVISION SUMMARY

- **Revises the Definitions section**
- **Adds a General Requirements section that centralizes new and existing general requirements**
- **Requires airport operators to use only Trusted Agents (TA) who have been fully vetted through TSA in the credentialing process, create an audit trail so that at any time TSA can determine which TA conducted enrollment and issued a credential to a worker, and provide an up-to-date list of all TAs at the airport to their Federal Security Director (FSD)**
- **Prohibits the airport operator from escorting a worker into the sterile area or Security Identification Display Area (SIDA) if the worker fails an STA**

SENSITIVE SECURITY INFORMATION

WARNING: THIS DOCUMENT CONTAINS SENSITIVE SECURITY INFORMATION THAT IS CONTROLLED UNDER 49 CFR PART 1520. NO PART OF THIS DOCUMENT MAY BE RELEASED TO PERSONS WITHOUT A NEED TO KNOW, AS DEFINED IN 49 CFR 1520, EXCEPT WITH THE WRITTEN PERMISSION OF THE ADMINISTRATOR OF THE TRANSPORTATION SECURITY ADMINISTRATION, WASHINGTON, DC 20560. UNAUTHORIZED RELEASE MAY RESULT IN CIVIL PENALTY OR OTHER ACTION. FOR U.S. GOVERNMENT AGENCIES, PUBLIC AVAILABILITY IS GOVERNED BY 5 U.S.C. 552.

SENSITIVE SECURITY INFORMATION

Security Directive 1542-04-8F
Page 2 of 14

- **Revises the Privacy Act Notice (Attachment A) for applicants and current identification media holders**
- **Requires direct employees of a Federal, State, or local government with unescorted access to non-public areas, except law enforcement officers, to undergo an STA and receive airport identification media**
- **Requires airport operators to conduct STAs and issue identification media to individuals with unescorted access to the air operations area (AOA)**
- **Requires airport operators to renew airport-issued identification media at least once every 2 years, beginning January 2009**
- **Requires airport operators to amend their airport security programs to include provisions that meet the Airport-Issued Media Audit Procedures and Signatory Training (Attachment B)**
- **Eliminates the requirement to check No Fly/Selectee Lists if the FSD determines that the airport operator has implemented the requirements in this SD**
- **Prohibits the airport-operator from authorizing entities to issue airport-approved ID media, except entities that hold TSA-approved or accepted security programs under 49 CFR Parts 1544 or 1546**
- **Amends the information airports must submit to TSA to initiate an STA**

APPLICABILITY: THIS SD APPLIES TO AIRPORT OPERATORS REQUIRED TO CARRY OUT A COMPLETE SECURITY PROGRAM UNDER TITLE 49 CODE OF FEDERAL REGULATIONS (CFR) SECTION 1542.103(a) AND AIRPORT OPERATORS REQUIRED TO CARRY OUT A SUPPORTING SECURITY PROGRAM UNDER TITLE 49 CFR SECTION 1542.103(b) THAT HAVE CHOSEN TO VOLUNTARILY INCLUDE SIDA OR STERILE AREAS IN THEIR AIRPORT SECURITY PROGRAMS.

ACTIONS REQUIRED: Each affected airport operator must implement the following measures **contained in this SD** in addition to the measures in the airport operator's TSA-approved security program and all current SDs.

I. **DEFINITIONS** (for this SD only):

- A. **"Airport-approved" identification media means media issued by an entity the airport operator has authorized to issue identification media under the airport's TSA-approved security program.**
- B. **"Airport-issued" identification media means media issued by an airport operator.**
- C. **"Applicant" means an individual who is applying for any identification media. The term "applicant" does NOT include direct employees of a Federal, State, or local government who are law enforcement officers and, as a condition of employment, have been subject to an employment investigation that includes a fingerprint-based Criminal History Records Check (CHRC).**
- D. **"Current media holder" means an individual who holds an airport-issued identification media as of the date of issuance of this SD.**

SENSITIVE SECURITY INFORMATION

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

- E. **"Identification media," "media," or "medium" means any credential, card, badge, or other media issued for identification purposes and use at the airport. This includes, but is not limited to, media signifying unescorted access to an air operations area (AOA), secured area, security identification display area (SIDA), sterile area, or to any public area. This also includes, but is not limited to, media issued to taxi drivers, parking lot attendants, vendors, and shuttle bus drivers. This does NOT include "visitor" media issued to individuals who must be under airport-approved escort to access the SIDA and/or sterile area on a limited-time or limited-use basis.**
- F. **"Security Threat Assessment" (STA) means a check conducted by TSA of databases relevant to confirming (1) that an individual does not pose a security threat, (2) that an individual possesses lawful status in the United States, and (3) an individual's identity.**
- G. **"Trusted Agent" (TA) means the airport operator employee or agent who collects information from applicants and current airport identification media holders used in the CHRC and STA, transmits the information to the Transportation Security Clearinghouse (TSCCH), authorizes the issuance of identification media, or issues the identification media.**
- H. **"Authorized to work" in the United States means an individual is a citizen or national of the United States, an alien lawfully admitted for permanent residence in the United States, or an alien authorized under the immigration laws of the United States to be hired, recruited, or referred for employment in the United States.**

II. GENERAL REQUIREMENTS

A. Airport-Issued Identification Media

1. Applicants

The airport operator may not issue identification media to an applicant or grant privileges that accompany issuance of the identification media until:

- a. **The airport operator has verified the identity and work authorization of the applicant as set forth in Section III. prior to submitting biographical information to TSA for an STA.**
- b. **The airport operator has completed a CHRC as set forth in Section VI. and 49 CFR Part 1542, where required.**
- c. **TSA has completed an STA of the applicant.**
- d. **TSA has notified the airport operator that the applicant is eligible to hold identification media. The airport operator reviews results of STAs at <http://www.tsc-csc.com>.**

2. Current Media Holders

Effective 30 days from date of issuance of this SD, when renewal of identification media is required under the airport operator's security program, the airport operator:

- a. **Must verify the identity and work authorization of the individual as set forth in Section III. prior to submitting biographical information to TSA for an STA.**

- b. **Must submit to TSA all information required in Section V. for the individual's STA.**
- c. **May issue a renewal identification media upon completion of the requirements in Sections II.A.2.a. and II.A.2.b. and need not wait for TSA's STA determination.**

3. Applicants and Current Media Holders

Notwithstanding TSA's eligibility determination, the airport operator must not issue identification media to an applicant or current media holder if it has reason to believe the individual poses a security threat; does not have lawful presence in the United States; or does not provide satisfactory identity verification. The airport operator must immediately provide the information to TSA and attempt to resolve the issue.

4. Biometric Access Control Systems.

The TSA encourages the implementation and use of airport biometric access control systems aligned with FIPS 201 standards. Where practicable, airports should explore biometric access control systems and identity verification technologies that will enhance the airport's ability to reduce unauthorized access and verify user identity.

B. Airport-Approved Identification Media

Effective 90 days from the date of issuance of this SD, the airport operator may authorize only entities that hold TSA-approved or accepted security programs under 49 CFR Parts 1544 or 1546 to issue airport-approved identification media.

C. Identification Media and Security Threat Assessments in the Air Operations Area

- 1. **Except as set forth in Section II.C.3., the airport operator must:**
 - a. **Complete the requirements set forth in Sections II.A.1.a., c., and d. for each individual who works in or has unescorted access to the AOA, except an individual who holds an airport-approved identification media issued by an entity that holds a TSA-approved or accepted security program under 49 CFR Parts 1544 or 1546, and**
 - b. **Ensure that each individual who works in or has unescorted access to the AOA holds airport-issued identification media, except an individual who holds airport-approved identification media issued by an entity that holds a TSA-approved or accepted security program under 49 CFR Parts 1544 or 1546.**
- 2. **Airport operators must implement the requirements in Section II.C.1. in accordance with the following schedule:**
 - a. **March 1, 2009 -- Category X and I airports**
 - b. **April 30, 2009 -- Category II, III, and IV airports**
- 3. **The airport operator is not required to issue identification media to the following individuals with unescorted access to the AOA:**
 - a. **Those who hold personal identification media issued under an exclusive area agreements authorized in 49 CFR Parts 1544 and 1546, or**

- b. Those who TSA requires the airport operator, under its airport security program, to accept other forms of identification media as sufficient, such as for uniformed flightcrew members, Federal Aviation Administration Flight Standards inspectors, and TSA inspectors.

D. Media Renewal

1. **Effective 90 days from the date of issuance of this SD, the airport operator must renew all airport-issued identification media at least once every 2 years.**
2. **When renewing identification media, the airport operator must:**
 - a. **Retrieve and deactivate the expiring identification media**
 - b. **Require the media holder to review and update his or her biographical information required in Section V. with any changes and submit the new information to TSA**
 - c. **Issue and activate new identification media.**

E. Denial of Escorted or Unescorted Access

When an applicant fails to successfully complete an STA or CHRC, or is subsequently disqualified due to an STA or CHRC disqualifying offense, where required, the airport operator may not grant the applicant escorted or unescorted access to the SIDA, secured area, sterile area, or AOA.

F. STA Information Required

TSA will not initiate an STA of an applicant or current identification media holder until the airport operator submits all information required in Section V.

G. Media and Access Revocation

When revoking identification media, the airport operator must complete all of the following:

1. Revoke the electronic access authority that corresponds to the identification media
2. Retrieve identification media, unless it is impracticable to do so
3. Update the spreadsheet referenced in Section V.
4. Provide the TSA-prepared redress information to the affected individual.

H. "Do Not Issue" Requirements

When TSA provides a "Do Not Issue" STA status to the airport operator for an applicant, the airport operator must:

1. Not issue the applicant identification media
2. Update the spreadsheet referenced in Section V.
3. Provide the TSA-prepared redress information to the affected individual.

I. FSD Notification

The airport operator must notify its FSD immediately if it:

1. Has reason to believe that any part of the identification media system, including electronic or other records, unused stock, forms, and operational components, has been compromised such that the reliability of the system is diminished,

2. Revokes or denies an individual unescorted access to the SIDA, sterile area, AOA or an individual's identification media. This notification requirement does not apply to routine **administrative** situations such as the loss of individual identification media.

J. Notification of Loss of Eligibility

The airport operator must require employers, flight schools, and all other entities that sponsor individuals for identification media to inform the airport operator immediately if a current media holder no longer meets the requirements described in Section III.A. (for example, if a visa authorizing employment has expired).

K. Flight Training

If an applicant applies for identification media for flight training, the airport operator must confirm that TSA has authorized the flight school to provide training to the applicant, as described in CFR Part 1552, Subpart A.

L. Recordkeeping

The airport operator must maintain an electronic record, paper record, or a comparable **TSA-approved records verification system** of the documents described below for a minimum of 180 calendar days after revocation of the individual's identification media and provide them to TSA upon request:

1. **Identity verification and authorization to work documents as required in Section III.**
2. Identifying information required for an STA as required in Section V.A.
3. Results of the CHRC required in Section VI.
4. Certifications required in Section VII.

M. No Fly and Selectee Lists Checks

1. **If the FSD determines that the airport operator has implemented the requirements of this SD, the airport operator is not required to conduct a name comparison of applicants and media holders against the Selectee and No Fly Lists as set forth in the SD-1542-01-10 series, except in the event of a system malfunction or failure in which the airport operator is unable to submit or retrieve STA information from the TSCH or TSA.**
2. **The airport operator has a continuing responsibility to implement the requirements of this SD in order to forego conducting the No Fly and Selectee Lists checks.**
3. **The airport operator must notify the FSD if it no longer implements a requirement in this SD and must resume conducting the No Fly and Selectee Lists checks at that time.**

N. Media Audit and Retrieval Procedures

Not later than 120 days from the date of issuance of this SD, the airport operator must amend its security program to include the minimum standards set forth in Attachment B.

O. Sterile Area Identification Media

The airport operator must ensure that each individual who works in the sterile area holds airport-issued identification media.

III. IDENTITY VERIFICATION and WORK AUTHORIZATION

When an STA is required, the airport operator must verify the applicant's or current media holder's identity and authorization to work by:

- A. Requiring the individual to present the identity and work authorization document(s) approved for use in the "Lists of Acceptable Documents" attached to the most current "Form I-9, Employment Eligibility Verification," issued by the U.S. Citizenship and Immigration Service (see www.uscis.gov/files/form/i-9.pdf)
- B. **Examining the document(s) to determine whether they appear to be genuine and relate directly to the individual presenting them.**

IV. TRUSTED AGENT ACCOUNTABILITY

Effective 60 days from date of issuance of this SD, except with respect to CHRCs and STAs conducted by an aircraft operator, the airport operator must:

- A. **Require that only TAs collect and transmit the biographical and biometric information used in the CHRC and STA, authorize the issuance of identification media, and issue the identification media.**
- B. **Establish and implement an auditable enrollment and media issuance process that identifies the TA who completes each task listed in Sections IV.B.1. through IV.B.3. To the extent practicable, TSA recommends that a TA should complete only one of these tasks for each applicant. Separation of duties in the credentialing process is considered a best practice to reduce the likelihood of fraud.**
 - 1. **The TA who collects and transmits the biographical and biometric information used in a CHRC and STA**
 - 2. **The TA who authorizes the issuance of the identification media**
 - 3. **The TA who issues the identification media.**
- C. **Complete a CHRC and STA of all TAs.**
- D. **Provide the list of TAs to its FSD.**
- E. **Update the list of TAs within 3 business days of any change or immediately when a TA's status or employment is suspended or revoked.**
- F. **Provide its FSD with the updated list of TAs as changes occur.**

V. INFORMATION REQUIRED FOR A TSA SECURITY THREAT ASSESSMENT

- A. **The airport operator must submit the following information, except as noted in Section V.A.5., to initiate an STA:**
 - 1. **Full legal name in this format: last name, first name, middle name.**
 - a. **Any other name used previously should also be provided. If providing another name, provide the given and surname.**

SENSITIVE SECURITY INFORMATION

Security Directive 1542-04-8F

Page 8 of 14

- b. **If no other name is applicable, leave the field blank.**
- c. **Do not supply the following in any of the name fields: none, N/A, NMN, or MNU.**
2. **Current mailing address**
3. **Daytime telephone number**
4. **Personal information:**
 - a. **Gender (M or F)**
 - b. **Date of birth (MMDDYYYY)**
 - c. **Country of birth [National Criminal Information Center (NCIC) 2-character abbreviation]**
 - d. **Citizenship country code (NCIC 2-character abbreviation).**
5. **Social Security Number (SSN) (9 digits, no dashes). (Providing the SSN to TSA is voluntary on the part of the applicant; however, failure to provide it may delay or prevent completion of the STA.)**
6. **For individuals who are not U.S. citizens, provide the:**
 - a. **Alien Registration Number (ARN) (9 digits, no dashes); or**
 - b. **I-94 Arrival/Departure Form Number (11 digits, no dashes).**
7. **For individuals who hold a non-immigrant visa, provide the visa control number, which appears in the top right-hand corner of the visa and is labeled "Control Number."**
8. **For individuals who are U.S. citizens born abroad or naturalized U.S. citizens, provide:**
 - a. **U.S. Passport number,**
 - b. **Certificate of Naturalization Number, which appears on the right side of the document and may be referred to as an ARN or INS number (9 digits, no dashes), or**
 - c. **Certification of Birth Abroad, Form DS-1350, or 10-digit document number, which appears in the top right-hand corner of the document. Precede the 10-digit number with DS (for example: DS 1234567890, do not include dashes).**
9. **Employer's name (the individual holds multiple identification media, list the employer associated with each medium.)**
10. **Airport information:**
 - a. **Airport 3-digit code, and**
 - b. **Airport category (X, I, II, III, or IV).**
11. **Identification media information:**
 - a. **Media number (except for new applicants)**
 - b. **Level(s) of access at the airport, such as SIDA, sterile area, AOA, secured area, or public area, indicating all that apply**
 - c. **Local media type (airport media type name)**

SENSITIVE SECURITY INFORMATION

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

SENSITIVE SECURITY INFORMATION

Security Directive 1542-04-8F

Page 9 of 14

- d. Media status (for example: active, not issued, revoked, pending, or suspended)
 - e. The date the status transaction occurred (that is: the date of application, issuance, or revocation in the following format: MMDDYYYY).
 - f. If revoked, the reason for revocation, such as lost, stolen, destroyed, terminated, expired, not returned, or otherwise unaccounted for.
- B. On a monthly basis, the airport operator must submit the information required in **Section V.A.** to the TSCH for each current **media holder** using the schedule provided below. If any of the days listed below fall on a weekend or Federal holiday, the information must be submitted on the next business day. If the airport badging office is not open on the day the submission is due, the information must be submitted on the next day the airport badging office is open.
- a. CAT X: 7th day of the month
 - b. CAT I: 14th day of the month
 - c. CAT II & CAT III: 21st day of the month
 - d. CAT IV (as applicable): 28th day of the month
- C. The information required in **Section V.** must be submitted to the TSCH in a Microsoft Excel spreadsheet or other method approved by the TSCH. The spreadsheet must be compressed as a .ZIP file and the compressed .ZIP file (not the spreadsheet) must be password protected. The file-naming convention for both the unprotected spreadsheet .XLS and the password-protected compressed .ZIP file is Airport Code_date (for example: ord_110306.zip and ord_110306.xls).
1. Submissions must be formatted according to the upload template provided by the TSCH. The template can be found on the secure TSCH website at <http://www.tsc-csc.com>. To access the template, login, select "Badging" from the left-side menu, and then select "Media Update Template." Improperly formatted submissions may be rejected for correction and resubmission.
 2. The completed template may be submitted to the TSCH by uploading through the secure TSCH website listed above or copied to compact disc (CD) and shipped by traceable means to the TSCH at:

Transportation Security Clearinghouse
601 Madison Street, Suite 400
Alexandria, VA 22314
 3. The airport operator must submit the password when uploading its file using the secure TSCH website. If the file is sent via CD, the password should be communicated using the "Contact Us" page at <http://www.tsc-csc.com/contact.cfm>. However, this could delay timely processing of files. If requested by the airport operator, the TSCH will provide a standard password for the airport operator to use for all submissions. The airport operator must use this password for each submission until a change is requested. Questions concerning the process should be directed to the "Contact Us" page or the TSCH at (703) 797-2550.

SENSITIVE SECURITY INFORMATION

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

- D. The airport operator must submit all routine **administrative** changes in the information required in **Section V.**, including all routine deletions, changes in media access level (such as from sterile area access to SIDA access), and reasons for change in media status to the TSCH no later than 3 business days following the airport operator's awareness of the change. **For changes to the status of airport-issued identification media** made for reasons of misconduct or where the individual was deemed to be a danger to themselves or others, the airport operator must report the change to the TSCH within 24 hours of the change.

VI. CRIMINAL HISTORY RECORDS CHECK

- A. The airport operator must comply with the following requirements for each applicant, except if the applicant is a direct employee of a Federal, State, or local government who requires unescorted access authority to the sterile area, and as a condition of employment was subjected to an employment investigation that included a CHRC.
- B. The airport operator must submit fingerprints to the TSCH for each applicant who requires unescorted access to the sterile area, except individuals who have already successfully completed a CHRC. The airport operator must submit the fingerprints no later than 72 hours after the date on which the fingerprints are provided by the applicant.
- C. The results of the CHRC may not be disseminated, except as provided for in 49 CFR Section 1542.209(j).
- D. All individuals awaiting results of a CHRC who need to access the sterile area must remain under continuous escort by an individual who has unescorted access authority to the sterile area.
- E. If the results of the CHRC preliminarily disclose a disqualifying criminal offense in accordance with 49 CFR Section 1542.209(d), the airport operator must ensure that the applicant remains under continuous escort by a current media holder who has unescorted access authority to the sterile area. **In addition**, the applicant must be referred to TSA for selectee screening at the screening checkpoint until the information is confirmed as inaccurate under established review procedures.

VII. CERTIFICATIONS

- A. **The airport operator must have applicants and current media holders read and sign the following certification when collecting information not already in the airport operator's records:**

"The information I have provided is true, complete, and correct to the best of my knowledge and belief and is provided in good faith. I understand that a knowing and willful false statement can be punished by fine or imprisonment or both (see Section 1001 of Title 18 of the United States Code)."

- B. **The airport operator must make the following certification available to applicants and current media holders for purposes of SSN verification:**

"I authorize the Social Security Administration to release my Social Security Number and full name to the Transportation Security Administration, Office of Transportation Threat Assessment and Credentialing (TTAC), Attention: Aviation Programs (TSA-19)/Aviation Worker Program, 601 South 12th Street, Arlington, VA 22202."

"I am the individual to whom the information applies and want this information released to verify that my SSN is correct. I know that if I make any representation that I know is false to obtain information from Social Security records, I could be punished by a fine or imprisonment or both."

"Signature: _____ Date of Birth: _____"

"SSN and Full Name: _____"

- C. The airport operator must present the Privacy Act Notice in Attachment A to each applicant and current media holder when they provide the information in Section V.**

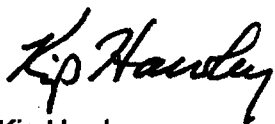
AIRPORT OPERATOR ACKNOWLEDGMENT: The airport operator must immediately provide written confirmation to the FSD indicating receipt of this SD.

AIRPORT OPERATOR DISSEMINATION REQUIRED: The airport operator must disseminate this SD to any law enforcement entity having 49 CFR Part 1542 responsibilities at that airport. Affected members of the Airport Law Enforcement Agency Network who currently have a memorandum of agreement with TSA will also receive this SD from TSA.

Dissemination to senior management personnel and supervisory security personnel must be on a strict need-to-know basis. No other dissemination may be made without prior approval of the Assistant Secretary for the Transportation Security Administration. Unauthorized dissemination of this document or information contained herein is prohibited by 49 CFR Part 1520 (see 69 Fed. Reg. 28066 (May 18, 2004)).

APPROVAL OF ALTERNATIVE MEASURES: With respect to the provisions of this SD, as stated in 49 CFR Section 1542.303(d), an airport operator may submit in writing to the Assistant Administrator for Transportation Sector Network Management, through the FSD, proposed alternative measures and the basis for submitting the alternative measures for approval. The Airport Operator must immediately notify the FSD whenever any procedures in this SD cannot be carried out by the airport operator or its agents.

FOR TSA ACTION ONLY: TSA must issue this SD immediately to affected 49 CFR Part 1542 airport operators and to the corporate security element of all affected aircraft operators and foreign air carriers.



Kip Hawley
Assistant Secretary

SENSITIVE SECURITY INFORMATION

Security Directive 1542-04-8F

Page 12 of 14

Attachment A

NOTE: This Privacy Act Notice should *not* be marked as Sensitive Security Information when issued to an individual.

Privacy Act Notice

Authority: 49 U.S.C. §§114, 44936 authorizes the collection of this information.

Purpose: The Department of Homeland Security (DHS) will use the biographical information to conduct a security threat assessment and will forward any fingerprint information to the Federal Bureau of Investigation to conduct a criminal history records check of individuals who are applying for, or who hold, an airport-issued identification media or who are applying to become a Trusted Agent of the airport operator. DHS will also transmit the fingerprints for enrollment into the US-VISIT's Automated Biometrics Identification System (IDENT). If you provide your Social Security Number (SSN), DHS may provide your name and SSN to the Social Security Administration (SSA) to compare that information against SSA's records to ensure the validity of your name and SSN.

Routine Uses: This information may be shared with third parties during the course of a security threat assessment, employment investigation, or adjudication of a waiver or appeal request to the extent necessary to obtain information pertinent to the assessment, investigation, or adjudication of your application or in accordance with the routine uses identified in the Transportation Security Threat Assessment System (T-STAS), DHS/TSA 002.

Disclosure: Furnishing this information (including your SSN) is voluntary; however, if you do not provide your SSN or any other information requested, DHS may be unable to complete your application for identification media.

SENSITIVE SECURITY INFORMATION

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

Attachment B

Airport-Issued Media Audit Procedures and Signatory Training

I. Airport-Issued Media Audit Procedures

The Transportation Security Administration (TSA) requires an amendment to your TSA-approved Airport Security Program (ASP) in accordance with 49 CFR 1542.105(c) that must include the procedures and language described below. Recent findings during regulatory inspections of compliance with 49 CFR 1542.211 have prompted the need for enhanced regulatory procedures and a revision to all ASPs for each Category X, I, II, III, and IV airport with a SIDA area.

A. Each ASP must include the following language, including the specific airport information, as appropriate:

"[Airport Name] has a verifiable system, inclusive of traceable documentation, that requires aircraft operators, foreign air carriers, tenants, and any other individuals in possession of airport-issued identification media to immediately notify the Airport Security Coordinator (or stated designee) of lost, stolen, and/or terminated media. A comprehensive description of this system is appended with this security program in Section [#]."

B. This verifiable audit system must include the requirements described below prior to being approved by the respective FSD. The audit system must apply to all airport-issued identification media. Within this system, the airport operator must:

1. Complete a comprehensive audit of all airport-issued identification media at least once every 12 months, and not less than 10 percent of the identification media via random selection every 6 months. This audit includes, but is not limited to, a comparison of the current list of airport-issued identification media holders against the lists maintained by those with signatory authority to identify and resolve any discrepancies. If more than 5 percent of all issued, unexpired identification media for any non-public area is lost, stolen, or otherwise unaccounted for, the airport operator must reissue identification media for that non-public area.
2. Minimize the number of individuals each aircraft operator, foreign air carrier, or tenant may authorize to certify SIDA media applications commensurate with the size and operation of the aircraft operator, foreign air carrier, or tenant to limit the opportunity for fraud. Upon review, TSA may determine that the number of authorized individuals must be reduced.

TSA recommends that the airport operator reduce the number of signatory authorities to the lowest number possible. This is considered a best practice to reduce the likelihood of fraud.
3. Ensure that all recordkeeping associated with the verification audit is retained for a minimum of 12 months and includes the date of completion, signature, and printed name of the verifying representative.
4. Ensure that any access rights associated with media that cannot be verified will be immediately deactivated or disabled.

5. Ensure that airport-issued identification media are configured or manufactured in a manner that reasonably discourages duplication and counterfeiting.
6. Ensure that media are deactivated when the airport operator becomes aware that media and associated access are no longer needed.

II. Signatory Authority Training

A. Each ASP must contain the following language:

"[Airport name] has a substantive training program for all persons designated as signatory authorities in the airport's identification media system that is verifiable through training completion records. The records are maintained by [the airport operator] at [location]. The training program and a template example of the completion record are appended to this security program at [location]."

B. Prior to receiving approval from the FSD to implement the training, the airport operator must ensure the training program:

1. Communicates clearly each signatory authority's responsibilities and duties
2. Provides all training recipients an opportunity to ask questions concerning their responsibilities
3. Requires all signatory authorities to certify they have completed and understand the training
4. Administers the training annually to each signatory authority
5. Retains all recordkeeping associated with the training program for a minimum of 12 months and includes the date of completion, signature, and printed name of the training administrator
6. Requires all signatory authorities to undergo an STA and CHRC before acting as a signatory
7. Requires all signatory authorities to complete the SIDA training.