

TSA AVIATION WORKER (AW) REQUEST COVER SHEET

FROM: Mr. Adnan Tikvesa
[REDACTED]
Atlanta, GA 30318

Daytime Telephone Number: _____
(Area Code)

DIRECTIONS FOR THE APPLICANT

Review and correct the above information as needed. After reviewing the above information and selecting from the options listed below, this cover sheet must be attached to the front of all documentation being submitted to TSA.

- EXTENSION OF TIME:** I will require more than 60 days to obtain documentation for my appeal.
- REQUEST FOR RELEASABLE MATERIALS:** I request a copy of my releasable materials.
- APPEAL:** I dispute the initial determination (an explanation must be provided).

Correspondence must be mailed via **U.S. Postal Service** to:

Kelly D. Wheaton
Assistant Chief Counsel
Threat Assessment and Internal Investigations
Transportation Security Administration
12th Floor – TSA 2
601 South 12th Street
Arlington, VA 20598

Please ensure that all documents provided for TSA's reconsideration of the initial eligibility assessment are attached. Closely following these directions will help ensure expedited processing of your request.



March 18, 2010

Kelly D. Wheaton
 Assistant Chief Counsel
 Threat Assessment and Internal Investigations
 Transportation Security Administration
 12th Floor – TSA 2
 601 South 12th Street
 Arlington, VA 20598

Dear Ms. Wheaton:

We write on behalf of our client, Adnan Tikvesa, an employee of Delta Airlines (Delta) at Atlanta Hartsfield International Airport. On November 12, 2009, an official of the Transportation Security Administration (TSA) served Mr. Tikvesa with an Initial Eligibility Determination Letter notifying him for the first time of TSA's determination that he "**may not** be eligible to hold an airport-approved and/or airport-issued personnel identification media" and its decision to immediately suspend the Secure Identification Display Area (SIDA) credential he had held since 2004. Exhibit A at 1 (emphasis in original). This decision was made without affording Mr. Tikvesa any notice of the basis for the determination, yet resulted in his immediate suspension without pay from his job as a Delta baggage service worker. Moreover, TSA's response to Mr. Tikvesa's request for materials providing the basis for the Initial Eligibility Determination is wholly inadequate, failing to notify him of any of the reasons underlying TSA's decision to revoke his SIDA credential. As a result, the appeals process fails to afford Mr. Tikvesa any meaningful opportunity to contest the Initial Eligibility Determination on the merits or to correct any misinformation underlying TSA's decision. This letter appeals the November 12, 2009 Initial Eligibility Determination; maintains that Mr. Tikvesa presents no threat to transportation security or national security and no threat of terrorism, and meets the standards that are required to maintain a SIDA credential; and challenges the due process deficiencies in both the Initial Eligibility Determination and the appeal process afforded to him. Mr. Tikvesa demands that TSA remedy its unconstitutional conduct and provide the reasons for its determination that he "may not be eligible" to hold a SIDA credential and evidence supporting these reasons so that he may appeal the determination on the merits.

Mr. Tikvesa is a 24-year-old US citizen who resides in Atlanta, Georgia. He first arrived in the United States in 1994 as a refugee fleeing the ethnic cleansing of Muslims in Mostar, a city in the former Yugoslavia,

AMERICAN CIVIL LIBERTIES
 UNION FOUNDATION
 LEGAL DEPARTMENT
 NATIONAL OFFICE
 125 BROAD STREET, 18TH FL.
 NEW YORK, NY 10004-2400
 T/212.549.2500
 F/212.549.2651
 WWW.ACLU.ORG

OFFICERS AND DIRECTORS
 SUSAN N. HERMAN
 PRESIDENT

ANTHONY D. ROMERO
 EXECUTIVE DIRECTOR

RICHARD ZACKS
 TREASURER

and became a naturalized United States citizen in 2003. Mr. Tikvesa has worked for Delta since October 2004 and was granted a SIDA credential for access to the secured areas of Atlanta Hartsfield International Airport (AHIA) in November 2004. His SIDA credential was renewed in April 2006 and again in April 2008. Mr. Tikvesa is part of a family that is proud to work for various employers in AHIA: his father works for Delta and holds a SIDA credential; his mother works for Delta Global Services and holds a SIDA credential; and his sister works for AHIA Customer Service. Mr. Tikvesa has never been convicted of, or even charged with, any crime.

On the morning of November 12, 2009, Mr. Tikvesa's supervisor, Mike Cousin, informed him that government officials wished to speak with him. He was taken to a room where he was met by officials of the TSA, U.S. Customs and Border Patrol, the Federal Bureau of Investigations, AHIA Operations, and Delta Airlines Corporate Security. At the meeting, a TSA official handed Mr. Tikvesa the Initial Eligibility Determination Letter. *See Exhibit A.* The same TSA official confiscated Mr. Tikvesa's SIDA badge and gave it to the official from AHIA Operations. An official from Delta Corporate Security asked Mr. Tikvesa to turn over his Delta personnel badge. None of the officials present provided Mr. Tikvesa any explanation for why TSA had determined that his clearance to access the secured area of the airport should be revoked.

Nor did the Initial Eligibility Determination Letter provide any explanation for TSA's decision. The letter stated that Mr. Tikvesa "**may not** be eligible to hold an airport-approved and/or airport-issued personnel identification media," that this determination was an "initial decision," and that Mr. Tikvesa had "not yet been permanently disqualified from holding an airport-approved and/or airport-issued personnel identification media." Exhibit A at 1 (emphasis in original). The letter indicated that Mr. Tikvesa had the option to "request a copy of the materials TSA used as the basis for making its initial decision" and to "file an appeal." *Id.* It also stated that the "TSA will not authorize an airport-approved and/or airport issued personnel identification media if TSA determines that an individual does not meet all Security Threat Assessment (STA) eligibility requirements." *Id.* The letter did not, however, notify Mr. Tikvesa that he did not meet the STA eligibility requirements or identify any specific requirement(s) not met by Mr. Tikvesa. Nor did the letter indicate whether Mr. Tikvesa was suspected by TSA of posing, or had been determined by TSA to pose, a security threat under 49 C.F.R. § 1540.201(c).

Moreover, although the Initial Eligibility Determination Letter directed Mr. Tikvesa to read the "Privacy Impact Assessment for the

Security Threat Assessment for Airport Badge and Credential Holders” (PIA) for “more information regarding STAs for an airport-approved and/or airport-issued personnel identification media,” Exhibit A at 1, the PIA itself does not identify any STA eligibility requirements, does not notify Mr. Tikvesa of the basis for the revocation of his SIDA credential, and does not identify any STA eligibility requirements not met by him. *See* Exhibit B. In short, nothing in the November 12, 2009 Initial Eligibility Determination Letter or the PIA indicates why or how the TSA determined that Mr. Tikvesa’s SIDA credential should be revoked.

Mr. Tikvesa wrote to TSA on November 19, 2009 to indicate that he was unaware of any reason for the suspension of his SIDA credential, to seek information as to why this decision was made, and to request all releasable and unreleasable materials underlying the Initial Eligibility Determination. *See* Exhibit C (Request Letter).

On January 19, 2010, TSA issued a wholly inadequate response to Mr. Tikvesa’s Request Letter. *See* Exhibit D (TSA Response). The TSA Response included three documents: (1) a one-page document detailing Mr. Tikvesa’s “Badge Applicant Details,” which provides his personal information (name, Social Security number, date of birth) and indicates that he was granted a SIDA badge; (2) a one-page “Cardholder Summary” listing Mr. Tikvesa’s identifying information (name, date of birth, residential address, Georgia driver’s license number) and his threat assessment, Fingerprint Clearance, Custom’s Clearance, and training dates; and (3) a heavily redacted two-page document entitled “Report of Investigation: Final” of the Investigations, Referrals and Analysis Division of the TSA Office of Transportation Threat Assessment and Credentialing. None of these documents offers any reasons for the revocation of Mr. Tikvesa’s SIDA credential. The “Report of Investigation: Final” document is so heavily redacted that it is impossible for Mr. Tikvesa to understand its contents. Exhibit D at 8-9. (In fact, the document does not contain a single sentence that is not redacted in part.) Although this document indicates that a “security threat investigation” of Mr. Tikvesa was initiated on June 18, 2009, it does not provide the reason for the initiation of the investigation, the process by which the investigation was conducted, or the results of the investigation. *Id.* As such, the document completely fails to provide Mr. Tikvesa any notice of the reasons underlying TSA’s decision to revoke his security clearance on November 12, 2009.

The Initial Eligibility Determination that Mr. Tikvesa “may not” be able to hold a SIDA credential took place without affording him any meaningful opportunity to contest the reasons for the determination.

Nevertheless, TSA's Initial Eligibility Determination resulted in the immediate suspension of Mr. Tikvesa's SIDA credential and his immediate suspension from his job without pay. Such action violates the "fundamental requirement of due process" that a person be granted "an opportunity to be heard at a meaningful time and in a meaningful manner" prior to being deprived of an interest. *Mathews v. Eldridge*, 424 U.S. 319, 333 (1976) (internal quotation marks omitted). Additionally, by failing to provide any basis for the Initial Eligibility Determination either at the November 12, 2009 meeting or in the Initial Eligibility Determination Letter, TSA failed to follow its own regulations, which require the provision of such information to an employee of an aircraft operator when an initial determination is made that the employee may not be eligible to hold a Security Identification Display Area credential due to failure to meet a requirement for such access. *See, e.g.*, 49 C.F.R. § 1540.205(d)(2)-(3) (requiring the provision of notice to an applicant of the "basis" for the initial determination that he does not meet security threat assessment standards set forth in TSA regulations); *id.* § 1544.229(h) (requiring the provision of notice to an applicant of the initial determination that he fails to satisfy the Criminal History Records Check requirement and provision of an opportunity to correct relevant records).

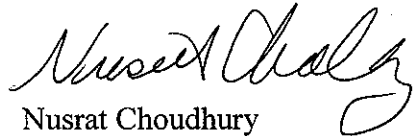
Moreover, although the Initial Eligibility Determination Letter stated that Mr. Tikvesa could appeal the Initial Eligibility Determination and request releasable materials to assist him with this appeal, even this process is constitutionally deficient. By failing to provide a single reason for its decision to revoke Mr. Tikvesa's security clearance and by so heavily redacting the paltry documents that it did provide, the TSA has failed to provide notice or a "meaningful" opportunity for Mr. Tikvesa to correct any misinformation or to contest the basis for TSA's decision to revoke his security clearance—a decision that has had and continues to have a profound impact on his ability to earn his livelihood. This failure also prevents him from utilizing the appeal process afforded by TSA regulations, which permits him to contest the basis for TSA's initial determination and to correct any misinformation. *See* 49 C.F.R. §§ 1515.5(b)(4), 1515.9(b) (permitting applicant to correct records where "the Initial Determination of Threat Assessment was based on a record that the applicant believes is erroneous"); *id.* §§ 1515.5(b)(5), 1515.9(b) (requiring applicant's reply to an initial determination of threat assessment to "include the rationale and information on which the applicant disputes TSA's Initial Determination"); *id.* § 1544.229(h) (providing applicant the opportunity to correct records underlying initial determination of failure to satisfy Criminal History Records Check).

Mr. Tikvesa continues to wonder why his SIDA credential was suddenly revoked after he had held it for more than four years, resulting in his inability to earn a living and to continue performing the job that he did so well. He maintains that he meets the standards that are required to maintain a SIDA credential, including security threat assessment standards. Mr. Tikvesa requests that TSA notify him of the reasons for its decision and provide him a meaningful opportunity to challenge these reasons. He is eager and willing to speak with TSA officials regarding any questions they may have about his eligibility to hold a SIDA credential.

Please direct a response to this appeal to Mr. Tikvesa, care of his attorneys at the addresses below.

AMERICAN CIVIL LIBERTIES
UNION FOUNDATION

Sincerely,



Nusrat Choudhury
Staff Attorney
American Civil Liberties Union
Foundation
125 Broad Street, 18th Floor
New York, NY 10004
(212) 519-7876



Azadeh Shahshahani
National Security/Immigrants' Rights
Project Director
ACLU Foundation of Georgia
1900 The Exchange SE, Suite 425
Atlanta, GA 30339
(770) 303-8111

Exhibit A

U.S. Department of Homeland Security
Office of Transportation Threat Assessment and
Credentialing
Arlington, VA 20598



Transportation
Security
Administration

TSA

Adnan Tikvesa

Atlanta, GA 30318

Re: Initial Determination of Eligibility

Dear Mr. Tikvesa:

The Transportation Security Administration (TSA) has determined that you may not be eligible to hold an airport-approved and/or airport-issued personnel identification media. This letter is not a final decision, but your Security Identification Display Area (SIDA) credential has been suspended until this matter is resolved. Instructions for preparing a response to this letter are included. TSA must receive your response within 60 calendar days after you receive this letter, or request for an extension of time to respond and TSA grants an extension. If you do not provide a response to TSA within 60 calendar days after you receive this letter or request an extension, TSA's decision regarding your eligibility determination will automatically become final and your airport operator will be notified that you are not eligible to hold an airport-approved and/or airport-issued personnel identification media.

RESULTS OF TSA'S INITIAL ELIGIBILITY ASSESSMENT:

After conducting the eligibility determination, TSA has made an initial decision that you may not be eligible to hold an airport-approved and/or airport-issued personnel identification media. TSA will not authorize an airport-approved and/or airport-issued personnel identification media if TSA determines that an individual does not meet all Security Threat Assessment (STA) eligibility requirements. For more information regarding STAs for an airport-approved and/or airport-issued personnel identification media, please refer to the Privacy Impact Assessment for the Security Threat Assessment for Airport Badge and Credential Holders at www.dhs.gov/privacy.

You have not yet been permanently disqualified from holding an airport-approved and/or airport-issued personnel identification media. This letter is an initial eligibility determination which notifies you of the decision made by TSA. The enclosure provided with this letter explains all options available to you when responding to TSA. You have the option to request an extension of time so that you may gather additional materials for your response/request a copy of the materials TSA used as the basis for making its initial decision, and/or file an appeal.

INSTRUCTIONS TO SEND INFORMATION TO TSA

The TSA Aviation Worker (AW) Request Cover Sheet **must** be attached to the front of all documentation and information being submitted to TSA. This cover sheet can be found at the end of the enclosed attachment and includes your full name, mailing address, daytime telephone number, airport information, and case number. Please change any information on the cover sheet that is incorrect and indicate the type of request you are submitting to TSA by selecting the appropriate request option(s).

Correspondence **must** be mailed to:

Transportation Security Administration
TTAC Aviation Programs (TSA-19)
601 S. 12th Street
Arlington, VA 20598

Use of the enclosed cover sheet and mailing correspondence to the above address is the fastest means of communicating with TSA. Use of overnight services (other than the U.S. Postal Service) will delay your correspondence.

You are not required to obtain an attorney. The enclosed attachment provides information on how to request releasable documents from TSA, submit an appeal, and/or request an extension of time.

TSA must receive your response within 60 calendar days of the date of this letter, unless you request and TSA grants an extension of time to respond. If you do not provide a response to TSA within 60 calendar days from the date of this letter or request an extension, TSA's decision regarding your initial eligibility determination will automatically become final and your airport operator will be notified that you are not eligible to hold an airport-approved and/or airport-issued personnel identification media. Please review the enclosure which provides detailed instructions on how to submit information to TSA. If you have any questions, please correspond in writing to the address provided.

Again, for more information regarding TSA eligibility determinations for an airport-approved and/or airport-issued personnel identification media, please refer to the Privacy Impact Assessment for the Security Threat Assessment for Airport Badge and Credential Holders at www.dhs.gov/privacy.

Sincerely,



Gale Rossides
Acting Administrator

Enclosure

HOW TO REQUEST RELEASABLE MATERIALS, SUBMIT AN APPEAL, AND/OR REQUEST AN EXTENSION OF TIME

CAN I REQUEST MATERIALS UPON WHICH THE ELIGIBILITY ASSESSMENT IS BASED?

Yes. You may request copies of the documents or information (releasable materials) that TSA used to determine that you may not be eligible to hold an airport-approved and/or airport-issued personnel identification media. This request must be typed or legibly written and submitted to TSA within 60 calendar days from the date the letter was issued.

TSA will provide you with a copy of the releasable materials no later than 60 calendar days after receiving your request, or a longer period as TSA may determine for good cause. TSA does not disclose classified information, as defined in Executive Order 12968, Section 1.1(d), and TSA reserves the right not to disclose any other information or material not warranting disclosure or protected from disclosure under law.

CAN I APPEAL THE ELIGIBILITY ASSESSMENT?

* Yes. You may submit an appeal (typed or legibly written) disputing TSA's initial determination, if you believe that you are eligible to hold an airport-approved and/or airport-issued personnel identification media. This appeal must include the reason(s) why you dispute TSA's decision and you must provide supporting documents to verify that you meet the eligibility requirements to hold an airport-approved and/or airport-issued personnel identification media. *

Other Eligibility Requirements: If your initial determination indicates that you do not meet the other eligibility requirements to hold an airport-approved and/or airport-issued personnel identification media based upon TSA's review of government databases or based upon other factors, you may submit documentation to establish your eligibility.

WHAT IS THE TIME FRAME FOR AN APPEAL?

You must send your appeal request to TSA within 60 calendar days of the date of:

- TSA's initial eligibility determination; or
- TSA's response to your request for releasable materials, if such a request was made.

If your appeal is approved, TSA will notify the airport operator within 60 calendar days of receipt of your appeal request that you are eligible to hold an airport-approved and/or airport-issued personnel identification media. If your request is denied, you will receive a Final Determination letter from TSA, and your airport operator will be notified that you are not eligible to hold an airport-approved and/or airport-issued personnel identification media. Please note that for good cause, TSA may take longer than 60 calendar days to effect notification.

CAN I GET AN EXTENSION OF TIME?

If you need additional time in which to submit a request for documents, materials, information, and/or an appeal, you may seek an extension of time. A written request must be sent to TSA to the address provided below within 60 calendar days of the date of the initial eligibility determination letter. TSA will grant an extension of time if good cause is shown.

If the time period to submit a request for documents, materials, information, and/or an appeal has expired, you may send a written request describing why the failure to submit a request within the time limit was excusable. TSA will grant an extension of time after the expiration of the time period if good cause is shown.

WHERE DO I SEND MY REQUEST FOR DOCUMENTS, AND/OR EXTENSION OF TIME?

The TSA Aviation Worker (AW) Cover Sheet found at the end of this letter **must** be attached to the front of all documentation and information being submitted to TSA. Please provide your full name, mailing address, and daytime telephone number, and the name of the airport that submitted your application, and indicate the type of request you are submitting to TSA by selecting the appropriate request option(s).

All correspondence must be mailed via U.S. Postal Service to the below listed address:

Transportation Security Administration
TTAC Aviation Programs (TSA-19)
601 South 12th Street
Arlington, VA 20598

WHAT WILL HAPPEN IF I DO NOT REQUEST DOCUMENTS, AN APPEAL, AND/OR AN EXTENSION OF TIME?

If you take no further action, TSA's decision will automatically become final 60 calendar days from the issue date of the initial determination of eligibility letter, your application will be closed, and your airport operator will be notified that you are not eligible to hold an airport-approved and/or airport-issued personnel identification media.

TSA AVIATION WORKER (AW) REQUEST COVER SHEET

FROM: Adnan Tikvesa
[REDACTED]
Atlanta, GA 30318

Daytime Telephone Number: _____
(Area Code)

DIRECTIONS FOR THE APPLICANT

Review and correct the above information as needed. After reviewing the above information and selecting from the options listed below, this cover sheet must be attached to the front of all documentation being submitted to TSA.

- EXTENSION OF TIME:** I will require more than 60 days to obtain documentation for my appeal.
- REQUEST FOR RELEASABLE MATERIALS:** I request a copy of my releasable materials.
- APPEAL:** I dispute the initial determination (an explanation must be provided).

Correspondence must be mailed via **U.S. Postal Service** to:

Transportation Security Administration
TTAC Aviation Programs (TSA-19)
601 South 12th Street
Arlington, VA 20598

Please ensure that all documents provided for TSA's reconsideration of the initial eligibility assessment are attached. Closely following these directions will help ensure expedited processing of your request.

Exhibit B



Privacy Impact Assessment
for the

Security Threat Assessment for Airport Badge and Credential Holders

December 1, 2008

Contact Point

Douglas Hofsass

**Acting General Manager, Commercial Airports
Transportation Sector Network Management
Transportation Security Administration
Douglas.Hofsass@dhs.gov**

Reviewing Officials

Peter Pietra

**Director, Privacy Policy and Compliance
Transportation Security Administration
TSAPrivacy@dhs.gov**

Hugo Teufel III

**Chief Privacy Officer
Department of Homeland Security
Privacy@dhs.gov**



Abstract

The Transportation Security Administration (TSA) is updating the Privacy Impact Assessment for the Security Threat Assessment (STA) for Airport Badge and Credential Holders to reflect an expansion of the covered population to include certain holders of airport approved badges, holders of Air Operations Area (AOA) badges, and individuals working in airport badging offices, and to reflect the use of US-VISIT's Automated Biometrics Identification System (IDENT) database as part of the STA process, including enrollment of fingerprints in that database for recurring checks. This Privacy Impact Assessment (PIA) is an updated and amended version of the PIA originally published by TSA on June 15, 2004, and subsequently amended on August 19, 2005 and on December 20, 2006. The requirements addressed in the previous PIAs are still in effect, including the requirement to conduct name-based STAs on all individuals seeking or holding airport identification badges or credentials and the requirement to conduct fingerprint-based criminal history record checks (CHRCs) along with name-based checks on individuals seeking access to the Security Identification Display Area (SIDA) or Sterile Area of an airport.

Overview

TSA has the statutory responsibility for requiring by regulation "employment investigation[s], including a criminal history record check and a review of available law enforcement data bases and records of other governmental and international agencies" for individuals who have "unescorted access" to the secure areas of airports and aircraft. 49 USC §44936. In addition, TSA has statutory responsibility to assess threats to transportation. 49 USC §114. In order to facilitate the required "review of available law enforcement data bases and records of other governmental and international agencies," TSA requires name-based STAs for all individuals seeking or holding airport identification badges or credentials, regardless of the level of access to airport facilities, in order to identify potential or actual threats to transportation or national security. The name-based STA involves recurring checks against Federal terrorist, immigration, and law enforcement databases.

TSA implemented the criminal history record check requirement in regulations codified at 49 CFR parts 1542, 1544, and Security Directives requiring fingerprint-based CHRCs. In addition to undergoing the name-based STA, individuals seeking credentials authorizing unescorted access to sterile areas, secured areas, the AOA, and Security Identification Display Areas (SIDA) must undergo a fingerprint-based CHRC. In addition, individuals performing functions within airport badging offices (handling badge applicant information, authorizing or issuing badges) will also undergo a fingerprint-based CHRC. These individuals must submit their fingerprints to the sponsoring airport or aircraft operator who then sends the information to their service provider to aggregate the fingerprint data and convert any paper fingerprint cards into an electronic format. The service provider then sends the fingerprint information via secure email to TSA. TSA forwards the fingerprint information to the Federal Bureau of Investigation (FBI) to conduct a fingerprint-based CHRC. The results of the CHRC are returned through TSA to the airport for adjudication of the CHRC by the airport or aircraft operator.

With this update to the PIA, TSA will also now transmit these already collected fingerprints to US-VISIT for enrollment into IDENT for recurring checks against immigration, terrorism, and law enforcement databases held in IDENT. IDENT is a DHS-wide system for the storage and processing of biometric and



biographic information for DHS national security, law enforcement, immigration, intelligence, and other DHS mission-related functions.

Additionally, TSA is expanding the requirement for name-based STAs to include individuals who hold or are applying for any identification credential or badge issued by an entity approved by the airport to issue identification credentials or badges for entities holding TSA-approved or accepted security programs under 49 CFR parts 1544 or 1546. It does NOT include law enforcement officers, who, as a condition of employment, have been subjected to an employment investigation that includes a fingerprint-based Criminal History Records Check (CHRC). For example, an airport may approve the employee badge of a tenant company on the airport such as an air carrier operating an air cargo facility. Fingerprint-based checks will also be conducted for those individuals whose airport approved badge involves access to the sterile area, secure area, AOA or SIDA.

Because this update entails the collection of personally identifiable information (PII) from a new population and adds IDENT database checks as part of the STA process, the E-Government Act of 2002 requires that TSA conduct a PIA.

Section 1.0 Characterization of the Information

1.1 What information is collected, used, disseminated, or maintained in the system?

TSA collects the following information from individuals to conduct STAs: full name (last, first, middle as appearing on government-issued ID), other names used, gender, date of birth, place of birth, Social Security Number (SSN), home address, phone number, submitting entity (i.e., employer or prospective employer), fingerprints, citizenship, and, if applicable, passport number and country of issuance, alien registration number or Form I-94 Arrival/Departure Number, or certificate of naturalization number or certificate of birth abroad. In addition, individuals who must submit fingerprints will also provide race, height, weight, eye color, and hair color. TSA will also collect the results of STA.

1.2 What are the sources of the information in the system?

TSA collects the information provided by individuals to their airports. In addition, the system may also include information originating from the terrorism, immigration, or law enforcement databases queried as part of the STA, such as US-VISIT for IDENT checks.

1.3 Why is the information being collected, used, disseminated, or maintained?

The information is collected to conduct STAs on individuals to ensure they do not pose, and are not suspected of posing, a threat to transportation or national security.



1.4 How is the information collected?

The Airport Security Coordinator (ASC) as required by Title 49, Code of Federal Regulations (CFR) part 1542 submits the individual's information to TSA through a secure web-based application operated by a service provider used by the aviation industry. (ASCs at smaller airports may also submit hard-copy fingerprints to TSA via the enrollment aggregator.)

1.5 How will the information be checked for accuracy?

Information collected from individuals is presumed to be accurate. In addition, individuals have an opportunity to correct inaccurate information as part of the redress process. Further, the service provider to the aviation industry that aggregates the information ensures that biometric and biographic information is correctly matched. TSA also expects to verify the accuracy of SSN with the Social Security Administration.

1.6 What specific legal authorities, arrangements, and/or agreements defined the collection of information?

49 U.S.C. §114(f); 49 U.S.C. §44936; 31 U.S.C. §7701. TSA has issued regulations implementing this authority with reference to airports at 49 CFR part 1542.

1.7 Privacy Impact Analysis: Given the amount and type of data collected, discuss the privacy risks identified and how they were mitigated.

TSA collects data elements designed to assist in completing the STA. Based on its experience conducting STAs, TSA collects information used to match individuals against various databases containing different elements while reducing the number of false positives and false negatives. TSA also collects contact information so that TSA can communicate with the individual in the event there are any issues requiring redress. This updated PIA expanded the population covered, but collects the same types of data as previously collected. Privacy risks include the potential for loss or unauthorized access to information, which is mitigated by imposing administrative and technical limits on access to the information.

Section 2.0 Uses of the Information

2.1 Describe all the uses of information.

TSA uses biographic information collected from individuals described in Section 1.1 above to conduct name-based STAs of persons seeking airport badges or credentials to identify potential or actual threats to transportation or national security. The STA involves recurring checks against Federal terrorist, immigration, and law enforcement databases. In addition, individuals seeking credentials authorizing unescorted access to sterile areas, secured areas, AOA, and Security Identification Display Areas (SIDA) must submit their fingerprints to the sponsoring airport or aircraft operator who, in turn, sends this information



to their service provider to aggregate the fingerprint data and convert any paper fingerprint cards into an electronic format. The service provider then sends the information via secure email to TSA. TSA sends the fingerprint information to the Federal Bureau of investigation (FBI) to conduct a fingerprint-based CHRC. Adjudication of the CHRC is conducted by the airport. TSA will also transmit these already collected fingerprints to US VISIT to perform checks against immigration, terrorism and law enforcement databases held in IDENT. Additionally, TSA requires STAs for certain individuals with airport approved badges. Fingerprint-based checks will be conducted for those individuals whose airport approved badge involves access to the sterile area, secure area, or SIDA.

TSA will also share information with the Social Security Administration in order to confirm the validity of SSN provided by the individual. Individuals will be asked to expressly authorize the Social Security Administration to confirm the validity of the SSN.

When necessary, TSA will forward the name of any individual who poses or is suspected of posing a threat to transportation or national security to the appropriate intelligence, immigration, and/or law enforcement agency or agencies. In these cases, the agency analyzes the information, determines whether the individual poses or is suspected of posing a threat to transportation or national security and notifies TSA of the determination so TSA can facilitate an appropriate operational response or notification to the airport or aircraft operator. Additionally, the immigration, law enforcement, or intelligence agency may take appropriate action concerning the individual, depending on the information.

2.2 What types of tools are used to analyze data and what type of data may be produced?

TSA matches individual information against terrorism, law enforcement, and immigration databases. The data produced is an STA result or CHRC result.

2.3 If the system uses commercial or publicly available data please explain why and how it is used.

Commercial data is not used by this system, but it is anticipated that TSA may in the future require airports to conduct identity verification efforts that will include the use of commercial data. This PIA will be updated if commercial database checks are required. Publicly available information such as court records may be used on occasion to resolve individual status when criminal or immigration case disposition information is otherwise unavailable.

2.4 Privacy Impact Analysis: Describe any types of controls that may be in place to ensure that information is handled in accordance with the above described uses.

User access is limited to individuals with a need to know the information for purposes of the program or to conduct the STA.



Section 3.0 Retention

3.1 What information is retained?

TSA retains the biographic and biometric information, as well as the STA result.

3.2 How long is information retained?

TSA will retain the information in accordance with the National Archives and Records Administration (NARA) records schedule approved March 8, 2007, Transportation Threat Assessment and Credentialing. The approved NARA schedule contains the following dispositions:

- TSA will delete/destroy information contained in the Subject Database System one year after an individual's credential or access privilege granted based upon the STA is no longer valid. In addition, for those individuals who may originally have appeared to be a match to a government watch list, but are subsequently cleared as not posing a threat to transportation or national security, retained information will be deleted/destroyed seven years after completion of the STA, or one year after any credential or access privilege granted based on the STA is no longer valid, whichever is longer.
- Information contained in the Subject Database System on individuals that are actual matches to a government watch list or otherwise pose a threat to transportation or national security, will be deleted/destroyed ninety-nine years after completion of the STA, or seven years after TSA learns that the individual is deceased, whichever is shorter.

3.3 Has the retention schedule been approved by the component records officer and the National Archives and Records Administration (NARA)?

Yes, it was approved on March 8, 2007.

3.4 Privacy Impact Analysis: Please discuss the risks associated with the length of time data is retained and how those risks are mitigated.

TSA will retain these records in accordance with the records retention schedule approved by NARA. The retention schedule was developed to provide flexibility to accommodate continued facility access by the individual. TSA will delete the individual's information one year after it is notified by the airport that the individual's access is no longer valid. Individuals originally identified as a possible match but subsequently cleared will have their information retained for seven years in order to provide the maximum opportunity for redress or review.



Section 4.0 Internal Sharing and Disclosure

4.1 With which internal organization(s) is the information shared, what information is shared and for what purpose?

Information will be shared within DHS with those officials and employees who have a need for the information in the performance of their duties. In the ordinary course, it is expected that information will be shared within TSA with the Office of Transportation Threat Assessment and Credentialing (TTAC), Office of Intelligence in the event of a match or possible match, Office of Chief Counsel for enforcement action or other investigation, Office of Security Operations for operational response, and the Office of Transportation Security Network Management for program management. Information may also be shared with the TSA Office of Civil Rights and Civil Liberties, TSA Privacy Office, TSA Ombudsman, and TSA Legislative Affairs to respond to complaints or inquiries. All information will be shared in accordance with the provisions of the Privacy Act, 5 U.S.C. § 552a. It is also expected that information will be shared with U.S. Immigration & Customs Enforcement (ICE) and U.S. Citizenship & Immigration Service (USCIS) for immigration issues.

TSA will also share fingerprints and associated biographic information with DHS's Automated Biometric Identification System (IDENT) as part of the STA. Further information about IDENT can be found in the IDENT PIA published by US-VISIT and publicly available on the DHS website.

4.2 How is the information transmitted or disclosed?

Depending on the urgency, information may be transmitted electronically, in person, in paper format, via facsimile, or by telephone. In most cases, the data will be shared within DHS on the encrypted DHS information technology (IT) network.

4.3 Privacy Impact Analysis: Considering the extent of internal information sharing, discuss the privacy risks associated with the sharing and how they were mitigated.

Information is shared internally with those DHS employees and officials, including contractors, who have a need for the information in the performance of their duties. Privacy risks that personal information may be disclosed to unauthorized individuals is minimized using a set of layered privacy safeguards that include physical, technical, and administrative controls to protect personal information in the automated system, appropriate to its level of sensitivity. Privacy risks associated with sharing information with IDENT is mitigated by sharing in accordance with the Privacy Act and DHS/TSA 002 SORN, (Transportation Security Threat Assessment System) and by the system user limitations within the IDENT system identified in the IDENT PIA.



Section 5.0 External Sharing and Disclosure

5.1 With which external organization(s) is the information shared, what information is shared, and for what purpose?

The information will be shared with airports and their service providers who aggregate individual information to provide to TSA. The information will be shared with the FBI for criminal history records checks and with the Terrorist Screening Center to resolve potential watch list matches. TSA also may share the information it receives with Federal, State or local law enforcement, immigration, or intelligence agencies or other organizations, in accordance with the routine uses identified in the applicable Privacy Act systems of records notice (SORN), DHS/TSA 002, Transportation Security Threat Assessment System (TSTAS). This SORN was last published in the *Federal Register* on November 8, 2005, and can be found at 70 FR 67731-67735.

TSA will also share information with the Social Security Administration in order to confirm the validity of SSN provided by the individual. Individuals will be asked to expressly authorize the Social Security Administration to confirm the validity of the SSN.

5.2 Is the sharing of personally identifiable information outside the Department compatible with the original collection? If so, is it covered by an appropriate routine use in a SORN? If so, please describe. If not, please describe under what legal mechanism the program or system is allowed to share the personally identifiable information outside of DHS.

Yes, sharing of information outside the Department is compatible with the original collection. Sharing will be to identify individuals who may pose a risk to transportation or national security, or for purposes of issuing credentials or other benefit. All sharing of information outside of DHS is covered by the above referenced SORN.

5.3 How is the information shared outside the Department and what security measures safeguard its transmission?

Depending on the recipient and the urgency of the request or disclosure, the information may be transmitted or disclosed telephonically, electronically via a secure data network, via facsimile or via password-protected electronic mail.



5.4 Privacy Impact Analysis: Given the external sharing, explain the privacy risks identified and describe how they were mitigated.

TSA will share this information under the applicable provisions of the SORN and the Privacy Act. TSA mitigates attendant privacy risk by limiting the sharing of this information to those who have an official need to know the information.

Section 6.0 Notice

6.1 Was notice provided to the applicant prior to collection of information?

A Privacy Act Statement is provided to individuals at the time they submit their information to the appropriate entity. The publication of this PIA and the applicable SORN, DHS/TSA 002, Transportation Security Threat Assessment System, also serves to provide public notice of the collection, use and maintenance of this information.

6.2 Do applicants have the opportunity and/or right to decline to provide information?

The individual is notified that they have an opportunity and/or right to decline to provide the identifying information requested. However, failure to provide the required information will result in TSA declining to process the application or being unable to determine whether the individual poses a threat to transportation or national security, which will result in a denial of access privileges or access credentials for which the individual applied.

6.3 Do applicants have the right to consent to particular uses of the information? If so, how does the applicant exercise the right?

No.

6.4 Privacy Impact Analysis: Describe how notice is provided to applicants, and how the risks associated with applicants being unaware of the collection are mitigated.

Individuals are provided with notice that enables them to exercise informed consent prior to disclosing any information to TSA, and have the right to refuse to provide information. Collection of the requested information is overt and apparent to the individual. Fingerprints and biographic information shared with IDENT will be enrolled in the IDENT system and may be shared within DHS with those employees who have a need for the information in the course of performing their duties, and outside of DHS in accordance with the Privacy Act and TSA system of records DHS/TSA 002. The privacy risk



associated with sharing information with IDENT without notice to those individuals who have already provided information is mitigated because sharing internal to DHS for immigration purposes has previously been disclosed to individuals.

Section 7.0 Access, Redress and Correction

7.1 What are the procedures that allow applicants to gain access to their information?

Individuals may request releasable information by submitting a Freedom of Information Act/Privacy Act (FOIA/PA) request to TSA in writing by mail to the following address:

Transportation Security Administration
Freedom of Information Act Office, TSA-20
11th Floor, East Tower
601 South 12th Street
Arlington, VA 22202-4220

FOIA/PA requests may also be submitted by fax at 571-227-1406 or by or by email at FOIA.TSA@dhs.gov. The FOIA/PA request must contain the following information: Full Name, address and telephone number, and email address (optional). Please refer to the TSA FOIA web site (<http://www.tsa.gov/research/foia/index.shtm>).

In addition, individuals may request access to and amendment of their records through the redress process as explained in paragraph 7.2 below.

7.2 What are the procedures for correcting inaccurate or erroneous information?

If an individual is disqualified because of the criminal history records check, the individual must notify the airport in writing of his or her intent to correct any information believed to be inaccurate within 30 days of being advised of disqualifying information. The applicant is responsible for correcting information by contacting the law enforcement jurisdiction responsible for the information and must apply for redress from the airport.

If the applicant believes he or she has been wrongly identified as a security threat relative to the STA, TSA provides a redress process and information on how to obtain releasable materials. There may be information or materials that are classified or otherwise protected by law or regulation that TSA will not disclose. All requests for releasable materials and challenges to the STA, must be submitted to TSA's Office of Transportation Threat Assessment and Credentialing at the below address.

Transportation Security Administration
TSA AV WORKER
TSA-19



601 S. 12th Street
Arlington, VA 22202

If TSA is unable to confirm the validity of the SSN, the individual must work through the Social Security Administration to resolve any issue.

7.3 How are applicants notified of the procedures for correcting their information?

TSA may send adverse notification directly to the individual in writing, by letter, electronic mail message, or facsimile. At the time of an adverse notification to an individual, TSA includes the appropriate procedures for redress and correction of information.

7.4 If no formal redress is provided, what alternatives are available to the applicant?

A redress process is provided for individuals who believe that they have been wrongfully denied the airport area access privileges and/or credentials for which they applied.

7.5 Privacy Impact Analysis: Please discuss the privacy risks associated with the redress available to applicants and how those risks are mitigated.

Individuals may request access to or correction of their personal information pursuant to the redress process described in 7.2 and pursuant to the Freedom of Information Act and Privacy Act of 1974. Privacy risks associated with redress include the collection of additional information on the individual. Risks are mitigated by handling the information in the same way other data associated with the STA process are handled.

Section 8.0 Technical Access and Security

8.1 What procedures are in place to determine which users may access the system and are they documented?

TSA information systems are protected by systems of passwords, restricted access and other measures to mitigate the risk of unauthorized access to sensitive information.

8.2 Will Department contractors have access to the system?

Yes. Contractors hired by TSA to perform IT maintenance and security monitoring tasks have access to the systems to perform their official duties. Strict adherence to access control policies is automatically enforced by the system in coordination with and through oversight by TSA IT Security Officers. Additionally, TSA may use contract adjudicators to review STA information. All contractors performing this



work are subject to requirements for suitability and a background investigation as required by TSA Management Directive 1400.3, TSA Information Security Policy.

8.3 Describe what privacy training is provided to users either generally or specifically relevant to the program or system?

All government and contractor personnel are required to complete on-line TSA Privacy Training, which includes a discussion of Fair Information Practices (FIPs) and instructions on handling personally identifiable information in accordance with FIPs and TSA Privacy Policies. Compliance with this requirement is audited monthly by the TSA Privacy Officer. In addition, security training is provided which helps to raise the level of awareness for protecting personal information being processed. All IT security training is reported as required in the Federal Information Security Management Act of 2002, Pub.L.107-347 (FISMA). Individuals accessing the system must have any necessary background investigations and/or security clearances for access to sensitive information or secured facilities based on TSA security policies and procedures.

8.4 Has Certification & Accreditation been completed for the system or systems supporting the program?

Yes. Information in TSA's IT systems is safeguarded in accordance with FISMA, which establishes government-wide computer security and training standards for all persons associated with the management and operation of Federal computer systems. The TSA systems associated with this PIA are operating on the authority of the Designated Accrediting Authority (DAA). Certification and Accreditation for the Crew Vetting Platform was received on September 1, 2005, and for the Screening Gateway on December 2, 2005.

8.5 What auditing measures and technical safeguards are in place to prevent misuse of data?

TSA system logs are reviewed to ensure no unauthorized access has taken place. All IT systems are audited annually for IT security policy compliance and technical vulnerability by the TSA IT Security Office. TSA ensures the confidentiality, integrity and availability of the data through a defense in depth strategy. Use of firewalls, intrusion detection systems, virtual private networks, encryption, access controls, identity management and other technologies ensures that this program complies with all DHS Security requirements.



8.6 Privacy Impact Analysis: Given the sensitivity and scope of the information collected, as well as any information sharing conducted on the system, what privacy risks were identified and how do the security controls mitigate them?

Data on the system is secured in accordance with applicable Federal standards. Security controls are in place to protect the confidentiality, availability, and integrity of personal data, including role-based access controls that enforce a strict need to know policy. Physical access to the system is strictly controlled with the use of proximity badges and biometrics. The system is housed in a controlled computer center within a secure facility. In addition, administrative controls, such as periodic monitoring of logs and accounts, help to prevent and/or discover unauthorized access. Audit trails are maintained and monitored to track user access and unauthorized access attempts.

Section 9.0 Technology

9.1 What type of project is the program or system?

This program is a database matching program that seeks to determine whether individual individuals are identified in law enforcement, immigration, or intelligence databases as posing or potentially posing a threat to transportation or national security.

9.2 What stage of development is the system in and what project development lifecycle was used?

The programs assessed are operational. This PIA reflects the expansion of certain STA requirements to a larger population, and the enrollment of fingerprints within IDENT.

9.3 Does the project employ technology which may raise privacy concerns? If so please discuss their implementation.

No.

Approval Signature

Original signed and on file with the DHS Privacy Office.

Hugo Teufel III
Chief Privacy Officer
Department of Homeland Security

Exhibit C

Adnan Tikvesa

[REDACTED]
Atlanta, GA 30318

To Whom It May Concern;

I have been employed with Delta Air Lines since October 29, 2004 at Atlanta Hartsfield International airport. I have never been in any type of trouble at work or with the Law.

This letter is in response to the TSA ruling on my work eligibility. I would like to receive additional information on why my SIDA/Airport privileges have been suspended at this time. I am not aware of any reason why it should be suspended. Please send me a copy of my releasable, as well as the un-releasable, materials.

Thank you

Sincerely yours,

Adnan Tikvesa

Exhibit D

U.S. Department of Homeland Security
Arlington, Virginia 20598



Transportation
Security
Administration

JAN 19 2010

Mr. Adnan Tikvesa
[REDACTED]

Atlanta, GA 30318

Re: Releasable Materials

Dear Mr. Tikvesa:

On November 13, 2009, the Transportation Security Administration (TSA) issued to you an Initial Determination of Eligibility regarding your airport-approved and/or airport-issued personnel identification media. TSA has received your request to obtain copies of releasable materials upon which the Initial Determination of Eligibility was based. This letter serves as TSA's response to your request.

We have enclosed all of the materials that we are authorized to release and that you have not already received. TSA does not disclose classified information, as defined in Executive Order 12968 section 1.1(d). TSA further reserves the right to not provide any other information or material not warranting disclosure or protected from disclosure under law.

Should you chose to do so, you may submit to TSA a reply to the Initial Determination of Eligibility, no later than 60 calendar days after the date of service of this letter. This written reply should include any information that you believe TSA should consider in reviewing the basis for the Initial Determination of Eligibility.

You should serve all documents upon:

Kelly D. Wheaton
Assistant Chief Counsel
Threat Assessment and Internal Investigations
Transportation Security Administration
12th Floor – TSA 2
601 South 12th Street
Arlington, VA 20598

TSA continues to examine this matter and shall notify you of its decision shortly.

Sincerely,

A handwritten signature in black ink, appearing to read "Kelly D. Wheaton", followed by a large, stylized flourish consisting of several overlapping horizontal lines.

Kelly D. Wheaton
Assistant Chief Counsel

HOW TO REQUEST RELEASABLE MATERIALS, SUBMIT AN APPEAL, AND/OR REQUEST AN EXTENSION OF TIME

CAN I REQUEST MATERIALS UPON WHICH THE ELIGIBILITY ASSESSMENT IS BASED?

Yes. You may request copies of the documents or information (releasable materials) that TSA used to determine that you may not be eligible to hold an airport-approved and/or airport-issued personnel identification media. This request must be typed or legibly written and submitted to TSA within 60 calendar days from the date the letter was issued.

TSA will provide you with a copy of the releasable materials no later than 60 calendar days after receiving your request, or a longer period as TSA may determine for good cause. TSA does not disclose classified information, as defined in Executive Order 12968, Section 1.1(d), and TSA reserves the right not to disclose any other information or material not warranting disclosure or protected from disclosure under law.

CAN I APPEAL THE ELIGIBILITY ASSESSMENT?

Yes. You may submit an appeal (typed or legibly written) disputing TSA's initial determination, if you believe that you are eligible to hold an airport-approved and/or airport-issued personnel identification media. This appeal must include the reason(s) why you dispute TSA's decision and you must provide supporting documents to verify that you meet the eligibility requirements to hold an airport-approved and/or airport-issued personnel identification media.

Other Eligibility Requirements: If your initial determination indicates that you do not meet the other eligibility requirements to hold an airport-approved and/or airport-issued personnel identification media based upon TSA's review of government databases or based upon other factors, you may submit documentation to establish your eligibility.

WHAT IS THE TIME FRAME FOR AN APPEAL?

You must send your appeal request to TSA within 60 calendar days of the date of:

- TSA's initial eligibility determination; or
- TSA's response to your request for releasable materials, if such a request was made.

If your appeal is approved, TSA will notify the airport operator within 60 calendar days of receipt of your appeal request that you are eligible to hold an airport-approved and/or airport-issued personnel identification media. If your request is denied, you will receive a Final Determination letter from TSA, and your airport operator will be notified that you are not eligible to hold an airport-approved and/or airport-issued personnel identification media. Please note that for good cause, TSA may take longer than 60 calendar days to effect notification.

CAN I GET AN EXTENSION OF TIME?

If you need additional time in which to submit a request for documents, materials, information, and/or an appeal, you may seek an extension of time. A written request must be sent to TSA to the address provided below within 60 calendar days of the date of the initial eligibility determination letter. TSA will grant an extension of time if good cause is shown.

If the time period to submit a request for documents, materials, information, and/or an appeal has expired, you may send a written request describing why the failure to submit a request within the time limit was excusable. TSA will grant an extension of time after the expiration of the time period if good cause is shown.

WHERE DO I SEND MY REQUEST FOR DOCUMENTS, AND/OR EXTENSION OF TIME?

The TSA Aviation Worker (AW) Cover Sheet found at the end of this letter **must** be attached to the front of all documentation and information being submitted to TSA. Please provide your full name, mailing address, and daytime telephone number, and the name of the airport that submitted your application, and indicate the type of request you are submitting to TSA by selecting the appropriate request option(s).

All correspondence must be mailed via U.S. Postal Service to the below listed address:

Kelly D. Wheaton
Assistant Chief Counsel
Threat Assessment and Internal Investigations
Transportation Security Administration
12th Floor – TSA 2
601 South 12th Street
Arlington, VA 20598

WHAT WILL HAPPEN IF I DO NOT REQUEST DOCUMENTS, AN APPEAL, AND/OR AN EXTENSION OF TIME?

If you take no further action, TSA's decision will automatically become final 60 calendar days from the issue date of the initial determination of eligibility letter, your application will be closed, and your airport operator will be notified that you are not eligible to hold an airport-approved and/or airport-issued personnel identification media.

TSA AVIATION WORKER (AW) REQUEST COVER SHEET

FROM: Mr. Adnan Tikvesa
[REDACTED]
Atlanta, GA 30318

Daytime Telephone Number: _____
(Area Code)

DIRECTIONS FOR THE APPLICANT

Review and correct the above information as needed. After reviewing the above information and selecting from the options listed below, this cover sheet must be attached to the front of all documentation being submitted to TSA.

- EXTENSION OF TIME:** I will require more than 60 days to obtain documentation for my appeal.
- REQUEST FOR RELEASABLE MATERIALS:** I request a copy of my releasable materials.
- APPEAL:** I dispute the initial determination (an explanation must be provided).

Correspondence must be mailed via **U.S. Postal Service** to:

Kelly D. Wheaton
Assistant Chief Counsel
Threat Assessment and Internal Investigations
Transportation Security Administration
12th Floor – TSA 2
601 South 12th Street
Arlington, VA 20598

Please ensure that all documents provided for TSA's reconsideration of the initial eligibility assessment are attached. Closely following these directions will help ensure expedited processing of your request.

Cardholder Summary



Badge #: 420609
Name: TIKVESA, ADNAN
Company: DELTA - SIDA
Activated: 05/01/2008
Status: Active
Expires: 04/26/2010

BADGE LAST CHANGED: 05/01/2008

CLEARANCE DATES

THREAT ASSESSMENT DATE: 10/01/2007
FINGERPRINT CLEARANCE DATE: 04/05/2006
CUSTOM'S CLEARANCE DATE: 04/13/2008
CUSTOM SEAL: RED
ESCORT? NO

TRAINING DATES

SIDA TRAINING DATE: 04/14/2006; COMPANY
DRIVER'S TRAINING DATE: 04/14/2006; COMPANY

RESIDENTIAL ADDRESS:

██████████
ATLANTA, GA 30318
PH: 0

SUPPLEMENTAL INFORMATION

CITIZENSHIP: United States of America - US
PLACE OF BIRTH: Bosnia and Herzegovina
DATE OF BIRTH: ██████████
HEIGHT: 6-05 **WEIGHT:** 200

LICENSE INFORMATION:

GA ██████████
EXPIRES: 04/26/2008

~~SENSITIVE SECURITY INFORMATION~~

TRANSPORTATION SECURITY ADMINISTRATION
OFFICE OF TRANSPORTATION THREAT ASSESSMENT
AND CREDENTIALING
INVESTIGATIONS, REFERRALS AND ANALYSIS DIVISION

REPORT OF INVESTIGATION
FINAL

Case Number:
20090707-005109

Period of Investigation:
18 Jun 2009 – 6 Nov 2009

Subject of Investigation:

Name: TIKVESA, Adnan

DOB: [REDACTED]

SSN: [REDACTED]

Citizenship: United States

Credential/Privilege: Secure Identification Display Area (SIDA) Badge

Basis of Investigation:

On 18 Jun 2009, a security threat investigation was initiated based upon a [REDACTED] report received from the Transportation Security Administration (TSA), Office of Transportation Threat Assessment and Credentialing (TTAC), Colorado Springs Operations Center (CSOC) [REDACTED] regarding Aviation Worker (AVW) subject, Adnan TIKVESA. (Exhibit 1)

Summary of Investigation:

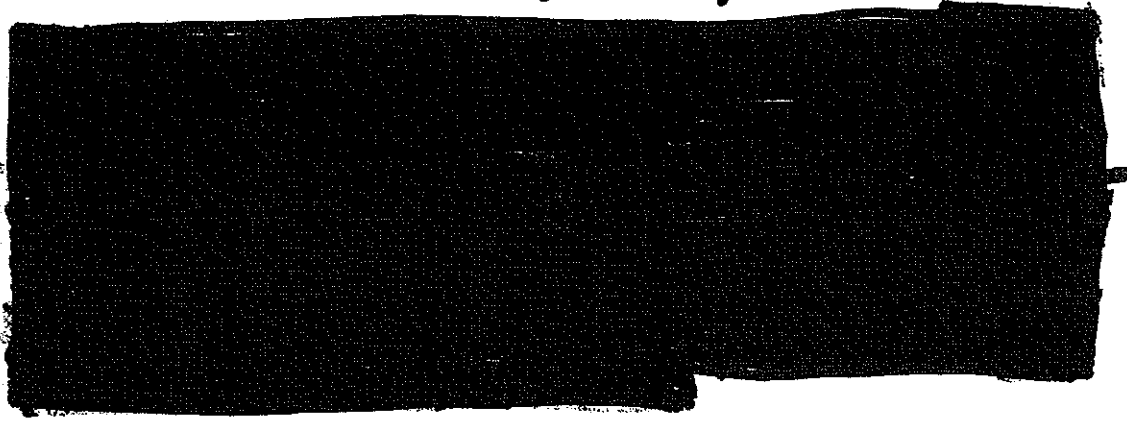
On 18 Jun 2009, [REDACTED] Atlanta Hartsfield International Airport (ATL), [REDACTED] was contacted and he advised that TIKVESA currently possess an ATL issued SIDA (420609), issued on 1 May 2009 and expiring on 26 Apr 2010. (Exhibit 2)

On 18 Jun 2009, TSA TTAC Adjudications Center [REDACTED] advised that TIKVESA's AVW application was received by the TTAC Adjudications Center on 16 Sep 2007, and was approved in the TTAC Consolidated Screening Gateway on 13 Aug 2008. (Exhibit 3)

On 18 Jun 2009, the TSA Office of Intelligence (OI) provided [REDACTED] [REDACTED] associated to TIKVESA and a threat assessment indicating the information [REDACTED] indicates that the individual is a threat to transportation and/or National Security. (Exhibits 4, 5)

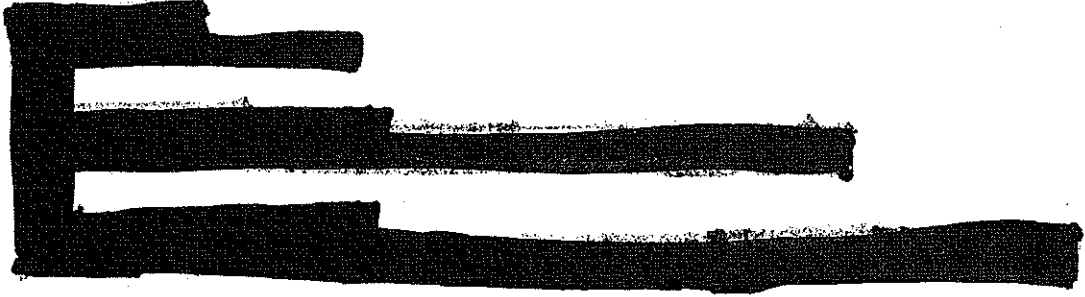
WARNING: This record contains Sensitive Security Information that is controlled under 49 CFR parts 15 and 1520. No part of this record may be disclosed to persons without a "need to know", as defined in 49 CFR parts 15 and 1520, except with the written permission of the Administrator of the Transportation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

~~SENSITIVE SECURITY INFORMATION~~





Conclusion:

Upon review of all information obtained during the investigation, TTAC determined that TIKVESA's TSA credential should be:



X Denied
(threat information justifies denial and there are no complicating factors)

Report Prepared By:  Date: _____
Report Reviewed By:  Date: _____
Approved for Action: _____ Date: _____

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