Privacy Impact Assessment
for the

Hazardous Materials Endorsement (Amended)

September 16, 2005

Contact Point
Lisa S. Dean
Privacy Officer
Transportation Security Administration
(571) 227-3947

Reviewing Official
Nuala O'Connor Kelly
Chief Privacy Officer
Department of Homeland Security
(571) 227-3813

Overview

This document amends the Privacy Impact Assessment (PIA) that the Transportation Security Administration (TSA) issued on January 26, 2005, concerning security threat assessments for drivers authorized to transport hazardous materials. TSA is providing two new electronic data transmission processes for the States to use to submit driver information needed to complete a security threat assessment to TSA. First, a State may access a secure website where it inputs required information and sends it to TSA directly. Second, the States may provide the information directly to TSA via secure file transfer in an XML file. These processes replace non-electronic transmissions, such as email, fax, or U.S. mail, which some States have been using. These new data transmission processes provide a more efficient, secure transmission of the data to TSA. This addition will improve the security of the system, and the efficacy of the security threat assessments for this program and should enhance the privacy of individuals who participate in this program.

This PIA applies to the systems and procedures TSA has implemented to conduct security threat assessments on individuals applying for, renewing, or transferring a Hazardous Materials Endorsement (HME) for a commercial driver's license (CDL). The Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act (USA PATRIOT Act) was enacted on October 25, 2001, and includes a provision that prohibits States from issuing, renewing, or transferring an HME until it is determined that an applicant does not pose a security threat. All commercially licensed drivers applying for, transferring, or renewing an HME are required to submit certain biographical and biometric information (such as fingerprints) as part of the application process. This information is used by TSA to conduct a security threat assessment. All applicants for an HME and those seeking to renew or transfer an HME are subject to the data collection requirements and the security threat assessment described in this document.

This PIA is amended and issued pursuant to the E-Government Act of 2002[1] in accordance with implementing guidance published by the Office of Management and Budget on September 26, 2003.[2]
To assist in reviewing this PIA, we provide the following list of frequently used acronyms and abbreviations.
AAMVAnet—Network maintained by the American Association of Motor Vehicle Administrators
CDL—Commercial drivers license
CHRC—Criminal history records check
DHS—Department of Homeland Security
DMS—Document Management System
DMV—Department of Motor Vehicles
DOT—U.S. Department of Transportation
FMCSA—Federal Motor Carrier Safety Administration
Gateway—Physical platform that houses software created and used by TSA's Office of Transportation Threat Assessment and Credentialing
HME—Hazardous materials endorsement
IRC—Intelligence-Related Check

[1] Pub.L 107-347, 44 U.S.C. Ch. 36 (December 17, 2002)
[2] *Guidance for Implementing the Privacy Provisions of the E-Government Act of 2002, Office of Management and Budget*, M-03-22 (September 26, 2003)

IFR—Interim Final Rule
RSPA—Research and Special Programs Administration
TSA—Transportation Security Administration
TTAC—TSA Office of Transportation Threat Assessment and Credentialing

2. Legislative and Rulemaking Overview

In response to the September 11, 2001 terrorist attacks, Congress passed several statutory mandates including the USA PATRIOT Act,[3] which, in part, provides that "A State may not issue to any individual a license to operate a motor vehicle transporting in commerce a hazardous material unless the Secretary of Transportation has first determined that the individual does not pose a security risk warranting denial of the license."[4]

Additionally, the Safe Explosives Act describes persons who may not lawfully "ship or transport any explosive in or affecting interstate or foreign commerce," to include any person under indictment for or convicted of a felony; a fugitive from justice; an unlawful user or addict of any controlled substance; any person adjudicated as a mental defective or committed to a mental institution; aliens, with certain limited exceptions; persons dishonorably discharged from the armed forces; and former U.S. citizens who have renounced their citizenship.[5] The U.S. Bureau of Alcohol, Tobacco, Firearms and Explosives (ATF) generally enforces these standards. However, the U.S. Department of Transportation (DOT) may displace ATF's authority by issuing regulations that address individuals engaged in the transportation of explosives.[6] In March 2003, DOT delegated the authority to carry out this provision to TSA.

To comply with the mandates of the USA PATRIOT Act and to trigger the exception for the transportation of explosives under the Safe Explosives Act, TSA issued an Interim Final Rule (IFR) on May 5, 2003 establishing security threat assessment standards for determining whether an individual poses a security threat warranting denial of an HME in coordination with agencies within DOT, the Federal Motor Carrier Safety Administration (FMCSA) and Research and Special Programs Administration (RSPA). [7] Additionally, TSA published an IFR on November 24, 2004,[8] that further describes the procedures the States, drivers, and TSA will follow.

[3] Pub. L. 107-56 (October 25, 2001), 115 Stat. 272, codified at 49 U.S.C. § 5103a.
[4] 49 USC 5103a(a)(1). The Secretary of Transportation delegated the authority to carry out the provisions of this section to TSA, which subsequently became part of the Department of Homeland Security (DHS). 68 FR 10988 (March 7, 2003).
[5] Pub. L. 107-296, November 25, 2002, 116 Stat. 2280, codified at 18 U.S.C. 842(i).
[6] 18 U.S.C. 845(a)(1).
[7] 68 FR 23852 (May 5, 2003). Also on May 5, 2003, two federal agencies within Department of Transportation and responsible for hazardous materials regulations, the Federal Motor Carrier Safety Administration (FMCSA) and the Research and Special Programs Administration (RSPA) issued Interim Final Rules (IFRs) creating standards to help ensure the safe transport of hazardous materials in the United States. On April 6, 2004, TSA issued a Final Rule that extended to January 31, 2005 the date by which all States must begin collecting fingerprints from HME applicants.
[8] 69 FR 68720 (November 24, 2004).

3. System Overview

3.1 What personally identifiable information will be collected?

A driver seeking to obtain, transfer, or renew an HME is required to complete a security threat assessment application (Application) and submit fingerprints and identifying information either to the State or to TSA's contractor in order for TSA to conduct a security threat assessment.

The identifying data collected on the Application and/or the fingerprint card includes: full legal name and any aliases; current residential address; mailing address if different than residential address; previous residential address; date of birth; social security number (voluntary, but recommended[9]); gender; height; weight; eye color; hair color; city, state and country of birth; immigration status and an alien registration number for both naturalized citizens and aliens; state of application; CDL number; military history, and if applicable, date of service and branch; and name and address of current employer(s). An applicant is also required to certify and acknowledge that he or she meets the standards for holding an HME as listed in 49 CFR §1572.5.

3.2 Why is this personally identifiable information being collected and what is the intended use of the information?

The information collected is used to conduct a security threat assessment as required by The USA PATRIOT Act on a commercial driver applying for, renewing, or transferring an HME. The security threat assessment will determine whether a person meets the standards required to hold or obtain an HME.

3.3 Who is affected by the collection of this data?

All drivers eligible to hold a CDL who are applying for, transferring, or renewing an HME will be affected. There are estimated to be approximately 2.7 million commercial drivers who hold an HME in the United States. On average, TSA estimates indicate that approximately 407,000 drivers each year will apply for a new HME, or transfer or renew their current HME.

3.4 What information technology system(s) will be used for this program and what is the step-by-step process for obtaining an applicant's data and conducting the security threat assessment?

To obtain, transfer, or renew an HME, a commercially licensed driver must undergo a security threat assessment to determine whether or not he or she poses a security threat. This security threat assessment consists of two types of background checks: 1) the intelligence-related check (IRC) that uses biographical information supplied by the driver to determine whether he or she meets the immigration standards or has a history of or connection to terrorist activity; and 2) the criminal history records check

[9] Although TSA does not require submission of a social security number, failure to provide it may result in delays in processing the application.

(CHRC) that uses fingerprints and biographical information to check for certain criminal convictions, any wants or warrants, and findings of mental incapacity.

In order to fully understand the process outlined below, it is important to understand the computer systems in place that manage the data. TSA created the Office of Transportation Threat Assessment and Credentialing Screening Gateway (Gateway) as a data aggregator. Applicant information is sent to the Gateway where queries are created and sent out to other systems that contain criminal, immigration, and terrorist-related data. If any of these systems contain data on the applicant, that system returns the information to the Gateway where it is aggregated and presented to TSA personnel for review. The Document Management System (DMS) is the companion system to the Gateway and facilitates the tasks of notifying applicants of the results of their security threat assessment and processing any appeals or waivers that may be submitted to TSA. The Gateway and the DMS do not, in and of themselves, require the collection or processing of personal information. The sole purpose of these systems is to provide the physical platform to house the software TSA's Office of Transportation Threat Assessment and Credentialing (TTAC) uses to complete security threat assessments.

3.4.1 Application

In the 34 jurisdictions that use TSA's contractor for fingerprint and information collection, drivers complete the Application at the contracotr's enrollment site and the contractor forwards the information to TSA in an XML file via secure file transfer. In the 17 jurisdictions that opted to conduct the collection without TSA's contractor, drivers complete the Application at State enrollment sites, and the State is responsible for forwarding the information to TSA.[10] TSA has permitted the States to transfer the Application data to TSA through non-electronic means, including fax, email, or U.S. mail. TSA then inputs the Application information into the Gateway. However, this process is expensive and time-consuming for TSA and the States. Therefore, TSA has developed two new electronic transmission methods for the States to use. The first is a secure website that contains the Application, which the States access through a secure connection and feeds directly into the Gateway. The second is State submission of an XML file containing driver information directly to TSA via secure file transfer (identical to method utilized by TSA's collection contractor). The website and the XML secure file transfer method are protected by the same systems and procedures that protect the Gateway. The States may continue to use the existing non-electronic system (fax, email and U.S. mail) to transmit data through September 30, 2005, but afterward, TSA will use the process only as a backup to the others.

A driver must also submit a set of fingerprints and other identifying information to the State or TSA's contractor, depending upon the procedures of the licensing State. For States that collect fingerprints, the State submits fingerprint information directly to the FBI. Otherwise, TSA's contractor collects and sends the fingerprints via secure file transfer protocol to the TSA clearinghouse, which then forwards them to the FBI over a secure network for a check against relevant criminal history record databases. Where TSA collects the fingerprints, TSA will retain the fingerprints to facilitate the potential for re-vetting at the appropriate time without the added burden of recollecting the fingerprints from the applicant.

[10] The States had planned to submit data to a network maintained by the American Association of Motor Vehicle Administrators (AAMVA), known as AAMVAnet, which is a secure system established to facilitate transfers of driver information among the States. However, AAMVAnet has not been implemented.

3.4.2 Security Threat Assessment

As required under TSA rules, no State can issue an HME unless an applicant for an HME has successfully completed a TSA security threat assessment. The HME security threat assessment includes a criminal history check (CHRC), and an intelligence check (IRC).

TSA determines that an individual poses a security threat if he or she: (1) is an alien (unless he or she is a lawful permanent resident or refugee, asylee, or other nonimmigrant authorized to work) or U.S. citizen who has renounced his or her U.S. citizenship; (2) is wanted or under indictment for certain felonies; (3) has a conviction for certain felonies within the preceding 7 years or was released from incarceration as a result of those felonies within the preceding 5 years; (4) is mentally incompetent or has been involuntarily committed to a mental institution; or (5) is considered to pose a security threat based on a review of pertinent databases.

Each phase of the security threat assessment is detailed below:

Fingerprint-based Criminal History Record Check

The CHRC involves the use of an applicant's fingerprints and biographical data to determine whether he or she has a disqualifying conviction or incarceration, outstanding warrant, or mental capacity issue. After the State or TSA submits an applicant's fingerprint information via secure file transfer to the FBI, the criminal history results are returned to TSA via secure file transfer protocol into theGateway. The Gateway is able to match the returned record to the appropriate driver. If the results indicate a potential disqualifying event, a TSA adjudicator reviews the record to determine if: (1) the record returned belongs to the applicant that the record was associated with, and (2) the record reveals any disqualifying factors. If the TSA adjudicator is unable to make a determination based solely on the record, the TSA adjudicator may access publicly available records (records accessible to anyone through physical search or the internet, such as local, county, state, and federal court records, voter registration, and residential addresses). For example, if a record indicates a conviction for a disqualifying offense but not the date of the conviction or the date of release from prison, the TSA adjudicator may access publicly available court or prison records to determine whether the conviction or release from prison falls within the applicable 7 or 5 year period.

On occasion, States may choose to provide TSA records from State databases relative to an applicant's criminal history for TSA to consider. This is not required by TSA, but TSA accommodates any State that chooses to provide such information to TSA in the proper format. If TSA receives the information in the proper format, a TSA adjudicator may review the State records and determine if the applicant has any disqualifying issues described in 49 CFR part 1572.

Intelligence-Related Check

As previously noted, TSA currently receives an applicant's biographical information in one of two ways. Biographical data collected by a TSA's contactor is sent electronically to the Gateway through a secure file transfer protocol. Biographical data collected by the States is currently sent to TSA via fax, email, or U.S. mail.

As discussed in detail above, TSA is now providing States with two alternative methods for transmitting data to TSA. The first is a secure website that contains the Application, and the second is submission of an XML file containing the driver information directly to TSA via secure file transfer (identical to method utilized by TSA's collection contractor). The website and the XML secure file transfer are protected by the same systems and procedures that protect the Gateway. In the IRC, the applicant

information is run against government and international databases related to citizenship and immigration status, and terrorist activity that TSA maintains or uses[11]. If records indicate that an applicant may not meet the security threat assessment standards, TSA adjudicators analyze available data further to ensure that it is not the result of a 'false positive' hit. TSA adjudicators have the appropriate clearances and training to ensure that the information is protected. After a thorough review of the underlying record(s), an adjudicator may determine that the applicant meets the security threat assessment standards. In such cases the applicant will be cleared. Alternatively, an adjudicator may determine that the results of the security threat assessment indicate that an applicant poses or is suspected of posing a security threat. If TSA determines that the applicant poses a security threat, TSA directs the State to revoke or deny the applicant's HME. In addition, if the applicant is under warrant or poses an immediate security threat, TSA notifies the appropriate law enforcement agency(ies) for remedial action. Based on TSA's assessment of intelligence, TSA may re-run the biographical data on all HME drivers through terrorist-related databases periodically as necessary.

3.4.3 Initial Determination

TSA uses the consolidated results of the IRC and CHRC to make an initial determination as to whether or not the applicant meets the security threat assessment standards. If an applicant meets the standards, TSA notifies the State and the applicant with a Determination of No Security Threat, thereby allowing the State to issue, transfer, or renew an HME.

If it is determined an applicant may pose a threat, TSA notifies the applicant with an Initial Determination of Threat Assessment (IDTA) containing the reason(s) for the issuance of the IDTA and directions as to how the applicant may apply for an extension of time, appeal or waiver. See Section 3.13 for details on the appeal and waiver. After an applicant's case has been adjudicated, the individual's case record is stored in the Gateway which serves as a repository for records and communications regarding the applicant. The Gateway also manages communications between TSA and the applicant to support a request for an extension of time, appeal or waiver. The system is covered by DHS/TSA-002 system of records notice. The electronic data transfer will be directly from the Gateway to the DMS database; as both databases reside in the same protected sub-network, the data is not accessible by any outside persons during the transfer. This sub-network is protected by a firewall, network and host-based intrusion detection software, and strict access controls including IDs and passwords.

If TSA determines that an applicant poses an immediate threat to national or transportation security or of terrorism, TSA issues an Initial Determination of Threat Assessment and Immediate Revocation. In this case, the State is instructed to immediately revoke the HME and the applicant is instructed to surrender the endorsement.

3.4.4 Final Determination

If an appeal of an Initial Determination is unsuccessful, TSA issues a Final Determination of Threat Assessment to both the State and the applicant. If an applicant chooses not to appeal, the Initial Determination converts to a Final Determination. The State is then required to deny or revoke the

[11] The biographic information used in such queries and the results are not separately maintained or used for other purposes by the federal government.

applicant's HME in accordance with TSA's procedures. In all cases, States are required to update the applicant's permanent DMV record with the status of the result of the security threat assessment.

3.4.5 Results of Security Threat Assessment

TSA currently provides the States with the results of the security threat assessments through email, fax, or U.S. mail. To provide a more efficient method of data transmission to the States, TSA is offering an alternative method to transfer this information. TSA will post results to each State's individual queue on a secure web interface with limited query functionality.

A State may access other State reports so long as the State of origin approves it and the user has a legitimate reason to access the information (such as to obtain information on a driver transferring into the State). State users will be presented with a 'log-in' screen and must authenticate their authority and need to access the data.

3.5 What notice or opportunities for consent are provided to individuals regarding the information collected and how that information is shared?

As noted above, TSA published Interim Final Rules on May 5, 2003, and November 24, 2004, which set forth the HME requirements.[12] In addition, a Privacy Act System of Records Notice was published, providing notice that TSA is collecting personally identifiable information relating to this program in the Transportation Security Threat Assessment System (T-STAS), DHS/TSA 002 system and setting out applicable routine disclosures.[13] Moreover, this PIA provides additional notice about the program.

As required by the Privacy Act, 5 U.S.C. 552a(e)(3), the HME Application includes a notice describing the authority for collecting this information, type of information to be collected, reasons for the collection of information, the consequences of failing to provide the requested information and how the information is used.

3.6 Does this program create a new system of records under the Privacy Act?

No. As stated above, this program is covered under T-STAS (DHS/TSA 002). The purpose of this system of records is to facilitate the performance of background investigations of transportation workers to ensure transportation security.

3.7 With whom will the collected information be shared?

The information is shared with the appropriate TSA and DHS employees and contractors involved in the program and other government agencies involved in the security threat assessment process. In addition, TSA may share information within DHS with those officials and employees who have a need for

[12] 68 FR 23852 (May 5, 2003); 69 FR 68720 (November 24, 2004).
[13] 69 Fed. Reg. 57349 – 57352 (September 24, 2004).

the record in the performance of their duties, including law enforcement components that need the information as part of law enforcement activities. For example, information may be shared with Immigration and Customs Enforcement for review of immigration status. If an applicant poses or is suspected of posing a security threat, then TSA will notify the appropriate law enforcement and/or intelligence agency(ies). State DMVs or other State agency responsible for granting an HME will also be notified as to whether an applicant may be issued an HME. TSA may notify an applicant's employer when a driver's HME has been revoked. In instances where a particular security need arises, additional information may be shared with employers in order to secure a particular facility.

3.8 How will the information be secured against unauthorized use?

TSA recognizes the sensitivity in providing personal information when applying for an HME and, therefore, has undertaken to secure this information using a series of procedural and information security safeguards. These safeguards ensure that the data collected is protected from unauthorized use as it moves through each point within the gateway system. Once an applicant's data is collected, it is transmitted via secure methods to government databases maintained or used by DHS for the security threat assessment screening.

After an applicant's case has been adjudicated, the individual's case record is stored in the Gateway, which serves as a repository for records and communications regarding the applicant. The Gateway also manages communications between TSA and the applicant to support a request for an extension of time, appeal or a waiver. Only TSA employees and contractors who have a need to know for purposes of conducting a security threat assessment, are authorized to access DMS.

TSA recognizes that the retention of personal information creates a general privacy and security risk. This risk, however, is mitigated by adhering to the Privacy Act, which protects personal information from unlawful disclosure, and the implementation guidance for Section 208 of the E-Government Act of 2002. Throughout the system requirements, appropriate processes for encryption and handling of data "at rest" and during transmission are followed to safeguard confidentiality, integrity and availability.

These safeguards are compliant with Federal Information Processing Standards listed below, TSA information security regulations, and corporate best practices. Specific safeguards used to secure the privacy data collected and maintained for the HME program are categorized in the following categories:

- Physical Security
  - Location of the gateway system at a secure TSA facility.
  - Controlled physical access to system servers and workstations.
  - Vetting government and contractor personnel by the TSA Office of Security.
- Data Security
  - Use of strong electronic data encryption at all system levels to prevent internal and external tampering of data and transmissions from all external sources.
  - Technical limitations on, and tracking of, data access and use.
  - Secure data transmission to prevent unauthorized internal and external access, including the use of password-protected e-mail for sending files among the sources used to conduct the security threat assessment.

- Password protection for files containing personal or security threat assessment data to prevent unauthorized internal and external access.

- Network Security
  - Use of secure telecommunications techniques.
  - Implementation of network firewalls to prevent intrusion into the HME network and associated databases.
  - Access controls in the form of user identification and password authentication to prevent access to security threat assessment systems by unauthorized users.
  - Use of security auditing tools to identify the source of failed gateway system access attempts by unauthorized users and the improper use of data by authorized operators.
  - Limitations on access to applicants' case files to only those with a "need to access" this information.

- Operations Security
  - Strict adherence to Federal Government security and information assurance policies, rules and regulations.
  - Strict adherence to TSA security and information assurance policies, rules and regulations.
  - Approval of HME security processes through TSA's formal System Security Accreditation process.

All HME data is handled under the guidelines of the following Federal security regulations and standards:

- *The Privacy Act of 1974*, which establishes minimum acceptable security and information collection practices for Federal computer systems.

- *CFR Title 49, Part 1520 - Protection of Sensitive Security Information*, which defines and requires the protection of "Sensitive Security Information" (SSI). SSI is sensitive but unclassified information related to transportation security that is provided to entities in the transportation sector on a need-to-know basis in order to carry out their security obligations.

- Federal Information Processing Standard (FIPS) 46-2 - Data Encryption Standard (DES), which defines the technical requirements for transmitting encrypted data at minimal acceptable levels of security (i.e., 56 bit encryption).

- FIPS 197 - Advanced Encryption Standard (AES), which defines the technical requirements for transmitting encrypted data at extremely high levels of security (i.e., 128 bit encryption and higher).

- FIPS 188 - Standard Security Label for Information Transfer, which defines the technical requirements for transmitting encrypted data across the internet using Secure Socket Layer (SSL). SSL is the accepted industry standard.

The Gateway system implements the aforementioned security technologies to ensure that all storage and transmission of data are safeguarded at appropriate levels of security. No classified information will be collected, processed, transmitted or stored by the Gateway or the DMS. It is also important to note that biometric storage and transmission of data are also safeguarded at appropriate levels of security.

Only TSA employees and contractors with proper access privileges are allowed access to this information to conduct security threat assessments. They will also receive appropriate privacy and security training and have any necessary background investigations and security clearances for access to sensitive or classified information and secured facilities. In order to obtain access to the TSA secure facility, personnel must be vetted by the TSA Office of Security and be subject to a risk assessment prior to connecting to the system. Moreover, TSA employees and contractors will be subject to the Rules of Behavior that clearly delineate the responsibilities and expected behavior of individuals accessing the system and consequences for non-compliance.

TSA's Privacy Officer is responsible for ensuring that the privacy of all applicants is respected and for responding to individual concerns about the collection and retention of personal information throughout the HME process. The TSA Privacy Officer will review privacy issues related to this program to ensure that privacy concerns are considered in all aspects of this program.

3.9 What technological mechanisms will be used to secure the data?

All applicant biographic data contained in the Application and provided by the applicant to support an appeal or waiver will be secured at all points in the system. No biometric data, specifically the fingerprints, will be collected by, transmitted to, commingled with or stored in the Gateway. Biometric storage will be accomplished via a secure stand-alone server. Appropriate processes for encryption and handling of data "at rest" and during transmission will be followed to safeguard confidentiality, integrity and availability.

- Encryption – All data transmitted between the internal and external systems for the IRC and CHRC searches are encrypted at 128 bit AES levels or are transmitted across SSL connection. Decryption keys are stored on a database at a different location that is protected by several firewalls.

- Audit Trails – Attempts to access sensitive data will be recorded for forensic purposes if an unauthorized individual attempts to access the information contained in the system.

- Physical Security – Measures will be employed to protect facilities, material and information systems. These measures include: use of armed or unarmed security guards at sites, fire protection and system backups, hard-bolting or fastening of databases, servers, and workstations; and credential readers for internal and external site access.

- User Access – System users are only allowed access to information and features of the system appropriate for their level of job responsibility and security clearance. These rights are determined by the identification provided when authenticating (i.e. user identification) to the system.

The HME program maintains a Gateway System and Security Guide containing a complete security plan and a description of the system's accreditation process approved by TSA.

3.10 What databases will be used in the security threat assessment process?

As is discussed in greater detail in section 3.4 above, TSA and its contractors use government databases that include criminal history and immigration records, terrorist watch-lists, and other information relevant to determining whether an applicant poses or is suspected of posing a security threat or that confirm an applicant's identity or alien status. In addition, if a TSA adjudicator is unable to make a determination solely on the record, he or she may access publicly available records (i.e. local, county, state, and federal court records, voter registration, and residential addresses, etc.).

3.11 Will the information be retained, and if so, for what period of time?

The rule requires States to retain the original application in electronic or paper form for a period of one year from the date of submission.

Currently, TSA does not have a records retention schedule from the National Archives and Records Administration (NARA). TSA is in the process of developing a records retention schedule that would permit it to destroy these records after a determined period of time. Until NARA approves this records schedule, however, TSA does not have legal authority to dispose of these records.

3.12 How will a driver seek redress?

3.12.1 Appeals

Drivers who believe that they have been mistakenly identified as posing a security threat or that they meet the HME standards for other reasons have the opportunity to appeal an IDTA. This appeal must be submitted within 30 days after the date of service of the IDTA or 30 days from TSA's response to the driver's request for materials pertaining to the determination.[14] In the event of an open disposition the applicant has 45 days from the date of service in which to reply and clarify the disposition.

An applicant may appeal an IDTA by: 1) serving TSA with a written answer that includes relevant agency or court documents to verify the applicant's identity and correct errors in his or her records; or 2) requesting a copy of the documents on which TSA based the Initial Determination. However, no documents that are classified or otherwise protected by law can be released. TSA will release as much information to the applicant as permitted by law to provide for a meaningful appeal.

The appeal process consists of a review of the IDTA, the materials upon which the decision was based, the applicant's appeal materials and any other relevant information or material available to TSA. An appeal of an IDTA based on a criminal offense, immigration status or mental competency issue is reviewed and decided by the TSA Director or designee. When an Initial Determination is based on information that an applicant does not meet the standards set forth in §1572.107 because of terrorist activity, and the applicant appeals that decision, the Assistant Secretary or designee reviews the case and makes the Final

[14] The date of service is defined in the IFR as date of delivery of personal delivery, date shown on a certificate of service, 10 days from the date of mailing if there is no certificate of service or date of electronic transmission.

Determination. This adds a level of scrutiny to ensure that a sound decision is made. TSA specifically chose to add a higher level of scrutiny to these final determinations because they may be based on classified information that TSA cannot release to the applicant and these applicants are not eligible for waivers.

Upon review of the appeal, the Director or Assistant Secretary may overturn the initial determination and serve a Withdrawal of the Initial Determination on the applicant and a Determination of No Security threat on the issuing State. Conversely, if the Director or Assistant Secretary upholds an IDTA, TSA will issue a Final Determination of Threat Assessment to the applicant and the State.

3.12.2 Waivers

An applicant may apply for a waiver if he or she has a disqualifying criminal offense or has been declared mentally incompetent in the past. A waiver may be filed only after an applicant has undergone a security threat assessment but no later than 30 days after service of a Final Determination of Threat Assessment.

Those applicants who are associated with terrorists or terrorist activity or who are in the country illegally are not eligible for a waiver. In addition, drivers convicted of certain criminal offenses such as treason, espionage, or sedition, are not eligible for a waiver.

3.13 Will the staff working with the data have appropriate training and security clearances to handle the sensitivity of the information?

All TSA and assigned contractor staff receive mandated privacy training on the use and disclosure of personal data. Additionally, training is conducted concerning the handling of personal data specifically related to the hazmat security threat assessment. Staff members assigned to handle classified threat assessment information are required to obtain appropriate security clearances. Also, all staff must hold appropriate credentials for physical access to the sites housing the Gateway system and management applications. TSA contractors also hold appropriate facility security clearances.

Responsible Officials

Lisa S. Dean, Privacy Officer, Transportation Security Administration, 571-227-3947

Department of Homeland Security

Approval Signature Page

_____ September 16, 2005

Nuala O'Connor Kelly
Chief Privacy Officer
Department of Homeland Security