Transportation Security Administration

# PRIVACY IMPACT ASSESSMENT

## FOR

# HAZARDOUS MATERIALS ENDORSEMENT

January 26, 2005


**Point of Contact**

Lisa S. Dean

Privacy Officer

Transportation Security Administration

(571) 227-3947

**Reviewing Official**

Nuala O'Connor Kelly

Chief Privacy Officer

U.S. Department of Homeland Security

(202) 772-9848

# Hazardous Materials Endorsement
# Privacy Impact Assessment

## 1. Introduction

This Privacy Impact Assessment (PIA) applies to the systems and procedures implemented by the Transportation Security Administration (TSA) to conduct security threat assessments on individuals applying for, renewing or transferring a Hazardous Materials Endorsement (HME) for a commercial drivers license (CDL). This PIA is an updated and amended version of the PIA that the Transportation Security Administration issued on June 1, 2004. Specifically, this document provides further details about the States' requirements relating to this program beginning on January 31, 2005. It also discusses the processes for the intelligence-related check (IRC) and the fingerprint based criminal history record check (CHRC), which together comprise the security threat assessment. Both checks help ensure that individuals holding a hazardous materials endorsement (HME) do not pose a security risk to the nation's transportation system.

The Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act (USA PATRIOT Act) was enacted on October 25th, 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 or renewing an HME are required to submit certain biographical and biometric information (e.g., 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 an HME are subject to the data collection requirements and the security threat assessment described in this document.

This PIA is conducted and issued pursuant to the E-Government Act of 2002[1] implementing guidance published by the Office of Management and Budget on September 26, 2003.[2] It represents TSA program design to be implemented as of January 31, 2005.

## 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, requires that "A

---

[1] Pub.L 107-347

[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)

[3] Pub. L. 107-56 (October 25, 2001), 115 Stat. 272, codified at 49 U.S.C. § 5103a(a)(1).

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] However, if any aspect of the transportation of explosives via highway are regulated by the U.S. Department of Transportation and address the transportation security issues of persons engaged in a particular aspect of the safe transportation of explosive materials, then those persons are not subject to the Safe Explosives Act while engaged in the transportation of explosives in commerce.

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 in coordination with agencies within DOT, the Federal Motor Carrier Safety Administration (FMCSA) and Research and Special Programs Administration (RPSA). [6] Additionally, TSA published an Interim Final Rule on November 24, 2004 that establishes security threat assessment standards for determining whether an individual poses a security threat warranting denial of an HME.[7] This PIA describes the information collection and handling that is necessary to determine if a driver applying for an HME is a security threat.

# 3. System Overview

## 3.1 What personally identifiable information will be collected?

A driver seeking to obtain or renew an HME is required to complete a Security Threat Assessment application and submit fingerprints and identifying information either to the

---

[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.

[6] 68 FR 23852 (May 5, 2003). Also on May 5, 2003, two federal agencies within Department of Transportation and responsible for HAZMAT 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.

[7] 69 FR 68720 (November 24, 2004). .

State or to a TSA approved agent in order for TSA to conduct a security threat assessment.

The identifying data collected on the Security Threat Assessment 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, gender, height, weight, eye color, hair color, city, state and country of birth, immigration status and date of naturalization if a naturalized citizen, alien registration number if an alien, state of application, CDL number, military history if applicable (such 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 §1572.9 of the IFR.

## 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 to determine whether or not he or she poses a security risk. 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 holders of a CDL applying for, transferring or renewing an HME will be affected. Estimates indicate that there are approximately 2.7 million commercial drivers in the United States. On average, TSA estimates indicate that approximately 407,000 drivers each year will apply for a new HME 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?

In order to obtain or renew an HME to a CDL, a commercially licensed driver must undergo a security threat assessment to determine whether or not he or she poses a risk to the transportation of hazardous materials. This security threat assessment consists of two types of background checks: 1) the IRC that uses biographical and identifying information supplied by the applicant to determine whether a driver lacks mental capacity, meets the immigration standards, and does/does not have a history or connection to terrorist activity; and 2) the CHRC that uses biometric data, i.e. a set of fingerprints, and biographic identifying information to check for a criminal conviction.

**Application**

To initiate an HME, an applicant is required to complete a Security Threat Assessment application, provide TSA with certain identifying information and certify his or her eligibility for an HME. The applicant submits the application to either the State or a TSA approved agent. It is then forwarded to TSA via a dedicated network maintained by the American Association of Motor Vehicle Administrators (AAMVA) or via secure file

transfer protocol by TSA's agent. AAMVA already has systems established to facilitate transfers of biographical data between the States through its secure network, AAMVAnet.[8] This information is then received by TSA in the Office of Transportation Vetting and Credentialing (OTVC) Screening Gateway (Screening Gateway). Once the application is received, a unique case record for each applicant is established by TSA. For the IRC portion of the security threat assessment, TSA transmits the necessary elements required to conduct searches for potential terrorist activity, mental incompetence, and immigration status to databases used or maintained by TSA/DHS.

An applicant must also submit a set of fingerprints and other identifying information to either the State or a TSA approved agent, depending upon the procedures of the licensing State. For States that collect fingerprints, the State submits fingerprint information directly to the FBI. Otherwise, an approved TSA agent collects and sends the fingerprints via secure file transfer protocol to TSA clearinghouse, which then forwards them to the FBI over a secure network for a check against relevant criminal history record database. It is important to note that some States may not have the funding or manpower to implement the infrastructure changes necessary to directly collect and transmit fingerprint and biographical data to TSA. Those States may work with an approved agent of TSA to meet the data collection and transmission requirements. The approved agent of TSA collects the drivers' application information and fingerprints and sends the data directly to TSA. It is also noteworthy that in those instances where the fingerprints are collected by the TSA approved agent, the fingerprints will be retained by TSA or the TSA agent to facilitate the potential for revetting at the appropriate scheduled timeframe within the renewal cycle without the added burden or duplication in recollecting the fingerprints from the applicant.

**Security Threat Assessment**

As required under TSA rules, no State can issue an HME unless an applicant for an HME (new, renewal or transfer) has successfully completed a TSA security threat assessment. The HME security threat assessment is composed of three phases: a fingerprint-based check (CHRC), an intelligence-related check, and a final disposition.

TSA determines that an individual poses a security threat if he or she: (1) is an alien (unless he or she is a U.S. National; 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 in military or civilian court for certain felonies; (4) has been adjudicated as a

[8] A number of states that will be collecting the Security Threat Assessment application information have indicated to TSA that the necessary system enhancements to allow data transmission using the AAMVA proprietary data format may not be complete by January 31, 2005. To allow sufficient time for states to implement system upgrades, TSA will provide temporary alternative methods for data transfer to include secure file transfer protocol, secure fax, email or U.S. mail. TSA encourages states to utilize the most secure means of the alternate data transfer mechanism possible. Once received, TSA will take the necessary steps to manually input the Security Threat Assessment application information into the Screening Gateway.

mental defective or involuntary committed to a mental institution; or (5) is considered to pose a security threat based on a review of pertinent databases.

The CHRC involves the use of an applicant's biometric fingerprint to positively identify when an individual has a criminal history with a disqualifying conviction or warrant. The intelligence related check involves the use of an applicant's biographical and identification information to check for potential terrorist activity, immigration status, and mental incompetency. The final disposition is the process by which TSA makes a final determination. In both the CHRC and the IRC, an applicant's data will be run through the appropriate criminal, terrorist-related, and immigration databases.

Once TSA receives an applicant's biographical information, it is input into the Screening Gateway where the system will format the data and assign a unique identification number to the individual. This gateway system is specifically designed to assist TSA by formatting information into a usable format and query databases in order to conduct the security threat assessments on the applicants. The Screening Gateway is able to collect the results from these checks and match the relevant returned record to the appropriate individual (the HME applicant) to which the records relate. The Screening Gateway also provides a platform from which TSA adjudicators review the information and arrive at a recommendation for TSA decision makers to review and access electronically.

Each phase of the security threat assessment is detailed below:

Fingerprint - based Criminal History Record Check

The fingerprint-based CHRC is used to positively identify whether an individual has a disqualifying conviction or warrant. After the State or TSA submits an individual applicant's fingerprint information via secure file transfer to the FBI[9], the criminal history results are then returned by the FBI to TSA via secure file transfer protocol. The FBI does not maintain this fingerprint information. The information is only used to return criminal history record results to TSA and is then destroyed. This information is received into the Screening Gateway. The Screening Gateway is able to collect the results from the fingerprint-based CHRC and match the returned record to the appropriate driver to which the records relates. A TSA adjudicator will review the record contained in the Screening Gateway to determine if: (a) the record returned does in fact belong to the applicant that the record was associated with, and (b) the record reveals any disqualifying convictions or warrants.

Additionally, 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 will accommodate any State that chooses to provide it to TSA

[9] The biometric information and the results are not separately maintained or used for other purposes.

for use in the security threat assessment. If received in a paper format, TSA will scan the information into the TSA database and maintain the information with the electronic records associated with the HME applicant. In either case, a TSA adjudicator reviews the entire file of the applicant and determines if the individual has any disqualifying crimes or warrants described in 49 CFR section 1572.103.

Intelligence-Related Check

As previously noted, TSA will receive an applicant's biographical information in one of two ways. States that are directly collecting fingerprints will also collect an applicant's biographical data and send the data electronically to TSA via a dedicated circuit through AAMVAnet into the Screening Gateway. Biographical data collected via a TSA agent for the Security Threat Assessment application will be sent electronically to the Screening Gateway through a secure file transfer protocol. In either instance, this information will be run against immigration and terrorist-related databases that TSA maintains or uses[10]. Any individual who meets the minimum criteria established by TSA as a possible match will undergo further analysis and screening. This involves an extensive review by TSA adjudicators.[11] TSA adjudicators will have the appropriate clearances and training to ensure that the information is protected. This next level of review and analysis is designed to reduce as much as possible the number of "false positives." After a thorough review of the underlying record(s), an adjudicator may determine that 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 individual poses or is suspected of posing a security threat. A determination that someone poses or is suspected of posing a security threat is only made after the Director of OTVC (or his or her designee) reviews of such recommendation. The purpose of this process is to protect applicants from being incorrectly identified as a threat.

After this review, TSA will direct the State to revoke or deny the applicant's HME. In addition, if appropriate where the applicant is under warrant or poses an immediate security threat, TSA will notify the appropriate law enforcement agency(ies) for remedial action. Based on TSA security needs, TSA may re-run the biographical data through terrorist-related databases as necessary.

## 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 does not pose a threat, TSA notifies the State and the

---

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

[11] TSA contractors performing this function are required by law and contract to protect the privacy of these records.

applicant with a Determination of No Security Threat, thereby allowing the State to issue or renew an HME.

However, in the event a TSA adjudicator makes a recommendation that an individual poses or is suspected of posing a security risk, such action will trigger the electronic transfer of the information contained in the Screening Gateway related to that recommendation and the creation of an electronic case file in TSA's Document Management System (DMS). The purpose of the DMS is simply to help TSA manage its administrative functions for notifications of initial and final determinations and the appeals and waiver processes. The electronic data will be transferred directly from the Screening 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, by network-based and host-based intrusion detection software, and by implementation of strict access controls to include IDs and passwords.

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

Initial Determinations may be appealed. See Section 3.13 for appeal and waiver redress.

**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 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.

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

As noted, TSA published an Interim Final Rule on May 5, 2003, requesting comments, amended the rule on November 7, 2003 and on April 6, 2004, and published an Interim Final Rule on November 24, 2004 requesting comments.[12] In addition, a Privacy Act System of Records Notice was published on September 24, 2004, providing notice that TSA is collecting personally identifiable information relating to this program in the

[12] 68 FR 23852 (May 5, 2003); 68 FR 63033 (November 7, 2003); 69 FR 17696 (April 6, 2004); 69 FR 68720 (November 24, 2004).

Transportation Security Threat Assessment System (T-STAS), DHS/TSA 002 system.[13] Moreover, this PIA provides additional notice about the program.

As required by the Privacy Act, 5 USC 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, a Privacy Act system of records that was established on September 24, 2004. 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. If an applicant poses or is suspected of posing a security threat, then TSA may notify the appropriate law enforcement and intelligence agency(ies). State DMVs and agencies responsible for granting an HME will also be notified as to whether an applicant has met the security threat assessment standards and 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 may arise, additional information may be shared with employers in order to secure a particular facility. In all instances, the collection, maintenance and disclosure of information are in compliance with the Privacy Act and the published System of Records Notice.

## 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.

As discussed earlier, if an applicant is identified as a security threat, then the applicant's case record is forwarded to the DMS. The DMS serves as a repository for records and communications regarding the applicant. The DMS also manages all communication between TSA and the applicant to support a request for a time extension, an appeal or a waiver. Only TSA employees and contractors who have a "need to know," for

[13] 69 Fed. Reg. 57349 – 57352 (September 24, 2004).

purposes of conducting a security threat assessment, will be authorized to access the HME system including the 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.

Specifically, 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 security 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 and Computer Security Act of 1987,* which establish minimum acceptable security practices for Federal computer systems. [14]
- *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 World Wide Web 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 screening 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/or security clearances for access to sensitive or classified information or 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

[14] The Computer Security Act of 1987, Pub. L. 100-235 (January 8, 1988).

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 HME 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 HME system. 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.
- Network Firewall – Connection of the HME System to AAMVAnet for the purpose of transmitting application data is through a firewall connected to a dedicated leased line. This is a security requirement of AAMVA. Firewalls are also used to prevent intrusion into the Gateway system and databases.
- 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?

TSA or its contractors employ a number of databases including criminal history records, terrorist watchlists and related databases, international databases, and other databases 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, TSA will search immigration databases to determine alien status. Finally, TSA may review databases related to an applicant's dishonorable discharge and mental incompetence, if any.

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

TSA is considering a retention period for these records of at least five years, to coincide with the HME renewal term required by the Federal Motor Carrier Safety Administration (FMCSA).[15] States are required 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 Will the information collected be used for any purpose other than the one intended?

Information collected is used only for the purposes outlined, consistent with the Privacy Act of 1974 and the published System of Records Notice for the Transportation Security Threat Assessment System (T-STAS), DHS/TSA 002. Specifically, the information is used by and disclosed to TSA personnel and contractors or other agents as needed for the security threat assessment of an individual holding or applying for an HME; and to appropriate law enforcement or other government agencies as necessary to identify and respond to outstanding criminal warrants or potential threats to transportation security; and to employers in order to secure a particular facility.

## 3.13 How will a driver seek redress?

**Appeals**

Drivers who believe that they have been wrongly identified as posing a security threat and believe they meet the standards for the security threat assessment have the opportunity to appeal an Initial Determination of Threat Assessment. This appeal must be submitted within 30 days after the date of service of the Initial Determination of

[15] 69 FR at 23859, n. 21.

Threat Assessment or 30 days from TSA's response to the driver's request for materials pertaining to the determination.[16]

An applicant may appeal an Initial Determination of Threat Assessment by: 1) serving TSA with a written answer to the Initial Determination of Threat Assessment 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 Initial Determination of Threat Assessment, 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 Initial Determination of Threat Assessment based on a criminal offense, immigration status or mental competency is reviewed and decided by the TSA Director. When an Initial Determination is based on information that an applicant does not meet the standards set forth in §1572.107 of the IFR, the Assistant Secretary reviews and makes a Final Determination of an appeal. This adds an additional 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 Initial Determination of Threat, TSA will issue a Final Determination of Threat Assessment to the applicant and the State. For purposes of judicial review, the Final Determination constitutes a final TSA order. The State is then required to initiate action to deny or revoke the applicant's HME in accordance with TSA's procedures.

## 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 at any time 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.

[16] 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.

## 3.14 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 that relates to 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 also hold appropriate credentials for physical access to the sites housing the gateway system and management applications. TSA contractors also hold appropriate facility security clearances.

**For questions or comments, please contact:**

- Lisa S. Dean, Privacy Officer, Transportation Security Administration, 571-227-3947.
- Nuala O'Connor Kelly, Chief Privacy Officer, Department of Homeland Security, 202-772-9848.