Transportation
Security
Administration

Security Threat Assessment for Individuals Holding a Hazardous Materials Endorsement for a Commercial Driver's License

Revised Privacy Impact Assessment

June 1, 2004

Contact Point:

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

Security Threat Assessment for Individuals Holding a Hazardous Materials Endorsement for a Commercial Driver's License Privacy Impact Assessment

I. Introduction

This Privacy Impact Assessment (PIA) is an updated and amended version of the PIA that TSA issued on April 15, 2004. TSA has revised the operation of its security threat assessment for individuals holding a hazardous materials endorsement for a commercial driver's license (HAZMAT) to reflect changes based on experiences to date. These changes should benefit positively the privacy of affected individuals in the program. This name-based security threat assessment phase is expected to be completed in 2004, with the actual implementation of the program beginning in the first quarter of 2005. Prior to implementation of the final program, TSA will issue a new PIA informing the public of changes to the program and any resultant impact to personal privacy.

• Rulemaking Overview

On May 5, 2003, the Transportation Security Administration (TSA) issued an Interim Final Rule establishing security threat assessment standards for commercial drivers authorized to transport hazardous materials.[1] On April 6, 2004, TSA issued a final rule that established the date on which the fingerprint criminal history record checks and other portions of the program must begin.[2] The final rules implement several statutory mandates, including Sections 1121-23 of the Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act (Patriot Act),[3] which says 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." 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).

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; and aliens with certain limited exceptions.[4]

To comply with these mandates, TSA announced in its final rule that it would conduct name-based checks of drivers who are currently authorized to transport hazardous materials using first, terrorist-related databases and then criminal databases as well as immigration records to determine citizenship status. This Privacy Impact Assessment (PIA), conducted pursuant to the E-Government Act of 2002 (P.L. 107-347) and the accompanying guidelines issued by the Office of Management and Budget (OMB) on September 26, 2003, is based on the current design of the program and reflects the Privacy Act System of Records Notice, Transportation Workers Employment Investigations System (DHS/TSA 002), published in the Federal Register on August 18, 2003, regarding the collection of personally identifiable information for the purpose of conducting background checks.

[1] 68 Fed. Reg. 23852 (May 5, 2003).

[2] 69 Fed. Reg. 17969-01 (April 6, 2004).

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

[4] Pub.L. 107-296, November 25, 2002, 116 Stat. 2280.

II. System Overview

- **What information will be collected and used for this security threat assessment?**

A HAZMAT endorsement allows a commercial driver to haul hazardous materials, including certain explosives. All commercially licensed drivers with HAZMAT endorsements are subject to the data collection requirements described in this PIA.

The information to be collected consists of: full name (as well as any aliases), current and three previous home addresses, mailing address (if different from home address), date of birth, Social Security Number, gender, height, weight, eye color, hair color, issuing State, Commercial Driver's License number, HAZMAT endorsement type, place of birth, country of citizenship, and alien registration number. (States have been asked to provide as many of the data fields as they have available in their existing systems.) Additionally, in the event that the assessment identifies an individual as a match to a name from a terrorist-related database and the individual believes that such identification is in error, that individual may be required to submit fingerprints and other information to verify identity and disprove the adverse information.

The information to be used initially, however, consists only of the name and date of birth of a HAZMAT driver. In conducting the required threat assessment, if a name matches with a name that is in a terrorist-related database, then the other information will be used to verify the identity of the HAZMAT driver. In this way, TSA intends to protect the privacy of affected parties, by using only personally-identifiable information to the extent necessary to establish true identity.

- **Why is the information being collected and who is affected by the collection of this data?**

The information is being collected in order to perform a security threat assessment of individuals currently authorized to transport hazardous materials. All holders of a commercial driver's license with a hazardous materials endorsement will be affected by this security threat assessment Estimates indicate that there are approximately 2.7 million commercial drivers with a HAZMAT endorsement.

- **What information technology system(s) will be used for this program and how will they be integrated?**

For ease of administration, TSA is using the American Association of Motor Vehicle Administrators (AAMVA), an association that currently provides access to State licensing data to assist the States. AAMVA currently facilitates transfers of licensing data between the States. AAMVA is assisting TSA in collecting the necessary data from State DMVs in a time-effective and efficient manner for both TSA and the States. Using AAMVA allows for one point of contact instead of multiple ones, and also will allow AAMVA to format all the data received into one workable format for TSA. Working through a contractor specifically hired for this purpose -- who, by law and contract is subject to the Privacy Act -- TSA is collecting and maintaining the information in accordance with its Privacy Act System of Records Notice, DHS/TSA 002. AAMVA forwards this information via secured email to the TSA HAZMAT program contractor, LexisNexis, or its subcontractor, InfoZen, where it is stored on secured desktop/laptop machines. The program contractor forwards names and dates of birth via a secure method to the Bureau of Customs and Border Protection (CBP), a component of DHS, which runs this information through terrorist-related databases it maintains or uses. If any individual whose name and date of birth are submitted appears to meet the minimum criteria established by the CBP database as a possible match, that information will be forwarded to TSA for further screening, and a determination that the individual does not pose or is not suspected of posing a security threat. After TSA review, the name of any HAZMAT operator posing or suspected of posing a security threat will be forwarded to appropriate law enforcement agency(ies). TSA will continue this procedure throughout the remainder of the 2004 name-based security threat assessment phase of the program in order to ensure that any resultant information suggesting a connection between a HAZMAT driver and terrorist activities is as narrowly drawn as possible. The purpose is to add a layer of protection for those individuals who may be affected by the threat assessment process and to reduce as much as possible the number of "false positives" that may affect individuals whose names are submitted for the program.

- **What notice or opportunities for consent are provided to individuals regarding what information is collected, and how that information is shared?**

As noted above, TSA published an interim final rule on May 5, 2003, followed by a final rule on April 6, 2004, announcing its intention to conduct this program. In its Privacy Act System of Records notice DHS/TSA 002, TSA also provided notice that it is collecting personally-identifying information relating to the Transportation Workers Employment Investigations System. This PIA provides additional notice about the program. TSA intends to provide further notices to individuals in future phases of this program.

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

No. This program is covered under a Privacy Act system of records that was established in 2003 called the "Transportation Workers Employment Investigation System," or 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. The system of records notice was published in the Federal Register on August 18, 2003, and can be found at 68 Fed. Reg. 49496, 49498. TSA is in the process of amending this system of records to reflect information that TSA will use in the threat assessment in future phases of this program.

- **What is the intended use of the information collected?**

Information will be used for performing name-based security threat assessments of HAZMAT drivers.

- **With whom will the collected information be shared?**

The information will be shared with the appropriate DHS personnel and contractors involved in processing the background checks. If persons pose or are suspected of posing a security threat, then TSA will notify the appropriate law enforcement agency. The collection, maintenance, and disclosure of information will be in compliance with the Privacy Act and the published system of records notice.

- **How will the information be secured against unauthorized use? (What technological mechanism will be used to ensure security against hackers or malicious intent?)**

DHS will secure personal information against unauthorized use through the use of a layered security approach involving procedural and information security safeguards. Specific privacy safeguards can be categorized by the following means, which are described in greater detail elsewhere in this document:

  - Technical limitations on, and tracking of, data access and use;
  - Use of secure telecommunications techniques; and
  - Limitation of physical access to system databases and workstations.

This approach protects the information in accordance with the following requirements:

The Privacy Act of 1974, as amended, (5 USC 552a) which requires Federal agencies to establish appropriate administrative, technical and physical safeguards to insure the security and confidentiality of information protected by the Act.

Computer Security Act of 1987, (Public Law 100-235), which establishes minimum acceptable security practices for Federal computer systems.

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

TSA will maintain the data for follow-on background checks that will be conducted beginning in the summer of 2004 and continue through implementation of fingerprint-based checks in January 2005, which are required under a fully implemented HAZMAT security threat assessment program. TSA also intends to retain these records for a sufficient period of time to permit affected individuals an opportunity to pursue redress or appeal measures, as well as for program auditing purposes. TSA does not yet have approval from the National Archives and Records Administration (NARA) to destroy records pertaining to this program. 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. TSA has requested a short retention period for these records from NARA.

- **Will the information collected be used for any other purpose other than the one intended?**

Information collected will be used for the purpose of conducting HAZMAT security threat assessments. TSA ensures this via legal agreements with its contractor and internal privacy policy enforcement with TSA entities involved in processing the security assessments. TSA's collection, maintenance, and disclosure of this information will be in compliance with the Privacy Act and the published system of records notice.

- **How will the driver be able to seek redress?**

For purposes of this phase of the program, drivers who believe that they have been wrongly identified as a security threat will be given the opportunity to verify their identity and correct errors in their records by submitting fingerprints or corrected court documents. When the program is fully operational, the redress procedures found at 49 C.F.R. 1572.141 will be implemented. Before the program becomes fully operational, TSA will issue a new PIA that will describe this and other elements of the final program.

- **What databases will the names be run against?**

DHS will run the names against terrorist-related databases maintained or used by TSA, CBP and/or other agencies within DHS, in order to identify those that pose a threat to transportation security.

- **What is the step-by-step process of how the systems will work once the data has been input and what is the process for generating a response?**

AAMVA synthesizes information from the States that identifies drivers who possess HAZMAT endorsements and provides it to TSA through TSA's HAZMAT Program contractor. The contractor further reviews the data and performs a quality assurance function. The program contractor forwards names and dates of birth via a secure method to the Bureau of Customs and Border Protection (CBP), a component of DHS, which runs this information through terrorist-related databases it maintains or uses. If any individual whose name and date of birth are submitted appears to meet the minimum criteria established by the CBP database as a possible match, that information will be forwarded to TSA for further screening, identity verification, and a determination that the individual does not pose or is not suspected of posing a security threat. After TSA review, the name of any HAZMAT operator posing or suspected of posing a security threat will be forwarded to appropriate law enforcement agency(ies). TSA will continue this procedure throughout the remainder of the 2004 name-based security threat assessment phase of the program in order to ensure that any resultant information suggesting a connection between a HAZMAT driver and terrorist activities is as narrowly drawn as possible. As previously stated, the purpose is to add a layer of protection for those individuals who may be affected by the threat assessment process and to reduce as much as possible the number of "false positives" that may affect individuals whose names are submitted for the program.

The named-based security threat assessment (described above) is conducted by running the list of HAZMAT driver names against a series of terrorist-related databases. The results of the checks at each step of the process are received and reviewed by DHS HAZMAT program management and contractors for quality assurance and privacy protections.

- **What technical safeguards are in place to secure the data?**

DHS employs the following technical safeguards to secure data:

  - Use of advanced encryption technology to prevent internal and external tampering of CBP data and transmissions.

  - Secure data transmission, including the use of password-protected e-mail for sending files among the participants listed above, to prevent unauthorized internal and external access.

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

  - Network firewalls to prevent intrusion into DHS network and CBP databases.

  - User identification and password authentication to prevent access to security threat assessment systems by unauthorized users.

  - Security auditing tools to identify the source of failed CBP system access attempts by unauthorized users and the improper use of data by authorized operators.

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

All DHS and assigned contractor staff receive DHS-mandated privacy training on the use and disclosure of personal data. Additionally, training will be conducted that relates to the handling of personal data specifically related to the HAZMAT security threat assessment. Staff assigned to handle classified threat assessment information will be required to obtain appropriate security clearances.

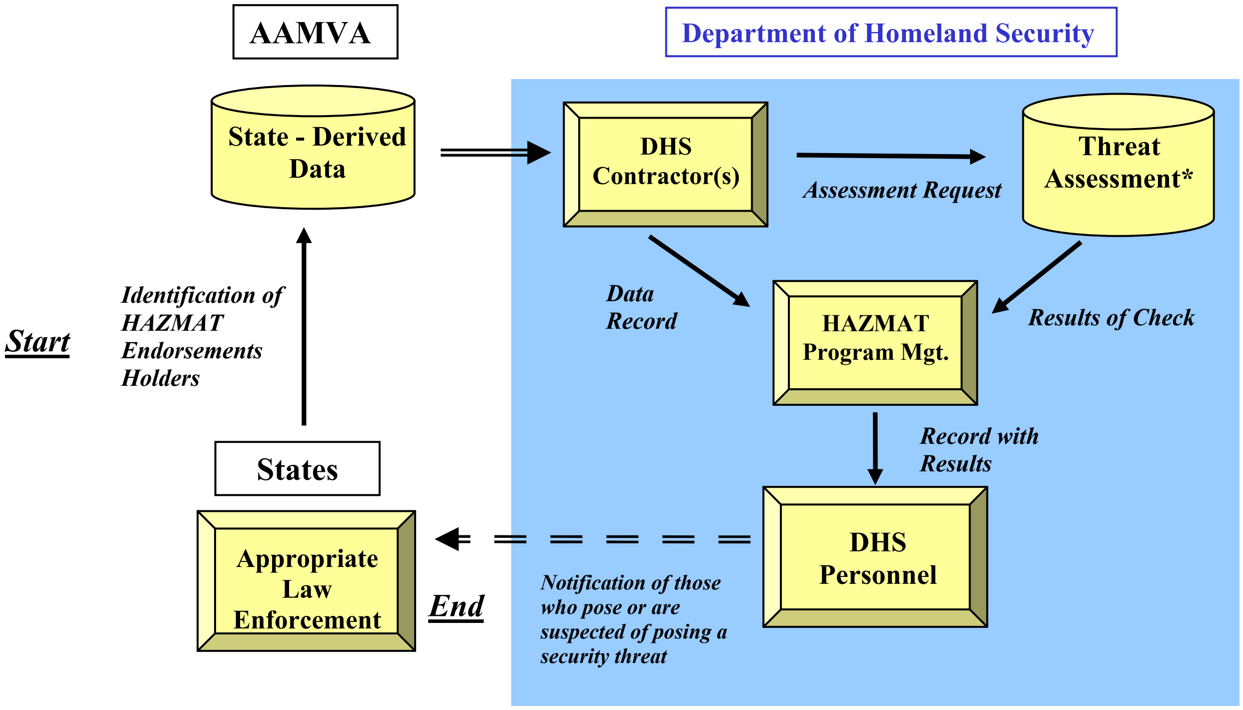
Additionally, all staff must hold appropriate credentials for physical access to the sites housing the security threat assessment databases and management applications. Physical access safeguards include the use of armed or unarmed security guards at sites; hard-bolting or fastening of databases, servers, and workstations; and credential readers for internal and external site access. The DHS 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

DHS HAZMAT Security Threat Assessment


AAMVA
Department of Homeland Security
State - Derived Data
DHS Contractor(s)
Assessment Request
Threat Assessment*
Start
Identification of HAZMAT Endorsements Holders
Data Record
HAZMAT Program Mgt.
Results of Check
Record with Results
States
Appropriate Law Enforcement
End
Notification of those who pose or are suspected of posing a security threat
DHS Personnel

* *Including Federal and Non-federal government data sources*