Privacy Impact Assessment
for
Universal Commercial Driver's License (CDL) Security Threat Assessment

October 12, 2007

Contact Point

Steve Sprague
Chief, Licensing & Infrastructure
TSNM Highway and Motor Carrier Security
Transportation Security Administration
(571) 227-1468

Reviewing Officials
Peter Pietra
Director, Privacy Policy and Compliance
Transportation Security Administration
TSAPrivacy@DHS.GOV

Hugo Teufel III
Chief Privacy Officer
Department of Homeland Security
Privacy@DHS.GOV

Abstract

The Transportation Security Administration (TSA) will conduct security threat assessments on Commercial Driver's License (CDL) holders. CDL holders are licensed to operate large commercial motor vehicles that potentially pose threats to transportation security. Congress directed TSA to perform threat assessments on certain CDL holders in the SAFE PORT Act Pub. L. No.109-347, 120 Stat. 1884 (2006). Since the potential threat extends beyond ports, TSA will perform security threat assessments on all CDL holders pursuant to its authority under 49 U.S.C. §114 (f) which gives TSA broad authority "to assess threats to transportation" including vetting persons who could pose a threat to transportation.

Introduction

TSA is responsible for assessing threats to transportation. While certain sub-populations of CDL holders currently undergo security threat assessments or other checks by TSA because they are covered under other TSA programs (such as Hazardous Materials Endorsement holders, Transportation Worker Identification Credential holders, airport Security Identification Display Area workers, and airport Sterile Area workers), the vast majority of CDL holders do not undergo a security threat assessment. TSA will perform a security threat assessment (STA) on CDL holders[1] by comparing individuals against Federal terrorism, immigration, and law enforcement databases. TSA will rely upon licensing data already collected by each state's (including the District of Columbia) licensing agency[2]. This data will vary among the various jurisdictions, but generally includes the CDL holders' full name; known aliases, social security number (if collected by the State); date of birth; place of birth; sex; height and weight; hair color; eye color; CDL number; driver's license number and state of licensure; current residential address; mailing address if different than residential address; previous residential address; and immigration status and alien registration number (if applicable). TSA does not require states to collect or provide information the states do not already collect.

If the CDL holder poses or is suspected of posing a threat to national or transportation security, [3] TSA will notify the driver by mail of the Initial Determination of Threat Assessment and provide the reason(s) for that determination and directions for how the driver may submit an appeal (as described more fully in Section 7.2). TSA's

[1] Some jurisdictions permit a CDL holder to remain active for a period of time after the CDL has expired, and renewal of the CDL during that period is typically a simpler process than the initial application or an application after the period has expired.

[2] The Federal Drivers Privacy Protection Act (18 USC §2721) permits disclosure of personal information from state drivers records to any government agency in carrying out its functions. Assessing security threats across all modes of transportation is a statutory function of TSA under 49 USC 114.

[3] In rare cases, an individual may be under investigation by other Federal agencies. In order not to compromise the investigation, TSA will not contact that individual or will not recommend revocation unless the threat is deemed to be imminent.

letter will notify the driver that if the driver's appeal is unsuccessful or if the driver does not respond in a timely manner, TSA's determination will become final. If there is a final determination of threat assessment, TSA may recommend to the U.S. Department of Transportation and the Governor of the licensing State that the driver's CDL be revoked.

Because this program entails a new analysis of information about members of the public in an identifiable form, the E-Government Act of 2002 requires that TSA conduct a Privacy Impact Assessment (PIA).

Section 1.0
Information collected and maintained

1.1 What information is to be collected?

TSA will rely upon licensing data for CDL holders and applicants collected by each state's (including the District of Columbia) licensing agency. TSA does not require any new information collection by the states. Data elements will vary among the various jurisdictions, but generally includes the CDL holders' full name; known aliases, social security number (if collected by the State); date of birth; place of birth; sex; height and weight; hair color; eye color; CDL number; driver's license number and state of licensure; current residential address; mailing address if different than residential address; previous residential address; and immigration status and alien registration number (if applicable)

1.2 From whom is information collected?

The information is being collected from state licensing agencies.

1.3 Why is the information being collected?

TSA is collecting the data to perform a security threat assessment and to communicate with the individual.

1.4 How is the information collected?

TSA is collecting this information from the state licensing agencies through password protected e-mail or CD.

1.5 What specific legal authorities/arrangements/agreements define the collection of information?

49 U.S.C. §114, and Section 125 of the Security and Accountability for Every Port Act of 2006 (SAFE Port Act), Pub. L. No.109-347, 120 Stat. 1884 (2006) authorize

this collection of information. In addition, TSA has entered into an MOU with Federal Motor Carrier Safety Administration (FMCSA defining data exchange and security measures to be implemented.

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

The information collected is information already existing within government databases. TSA is collecting sufficient personally identifiable information (PII) to minimize the likelihood that individuals will be falsely identified as being a match with a name on a Federal watch list. The privacy risks associated with this collection include the potential loss of PII. Risks have been mitigated through the security measures discussed in Sections 8.0 and 9.0 below.

Section 2.0
Uses of the system and the information

2.1 Describe all the uses of information.

TSA will use the information to conduct security threat assessments for the purpose of identifying actual or potential threats to transportation security. Due the resource constraints, an initial threat assessment will be performed by the Terrorist Screening Center on the current CDL holder population. In the future, it is expected that TSA will perform the security threat assessment. TSA will perform perpetual vetting of CDL holders and applicants. The results of the name-based check will be used to assess the security risks associated with the covered individual. If TSA determines that the individual may pose or poses a security threat, TSA may notify the individual that TSA has determined he or she may be a security threat. If TSA determines that the individual poses an imminent security threat, TSA may first contact appropriate law enforcement and State agencies, and may seek revocation of that driver's commercial driving privileges. The individual will have an opportunity to appeal TSA's determination in either case. If redress, appeals, and adjudication procedures do not change the substance of TSA's findings, TSA will issue a letter stating its determination is final and requesting that the driver surrender his or her commercial driver's license and cease all operation of a commercial vehicle. TSA will also recommend to the U.S. Department of Transportation that the driver's right to hold a CDL be denied; and will issue a similar recommendation to the governor of state that issued the CDL. In the event that TSA considers the driver to represent an "imminent threat" to transportation security, TSA may seek the immediate withdrawal of CDL privileges by the FMCSA or appropriate state governor while redress and adjudication proceedings are conducted.

2.2 Does the system analyze data to assist users in identifying previously unknown areas of note, concern, or pattern?

No.

2.3 How will the information collected from individuals or derived from the system be checked for accuracy?

Information is being provided from state licensing agencies. It is presumed that state commercial driver files contain accurate information. TSA expects that individuals provide accurate information to an official state licensing agency in order to obtain a commercial driver's license. I

Information may be collected directly from the individual in connection with an appeal of an IDTA.

2.4 Privacy Impact Analysis: Given the amount and type of information collected, describe any types of controls that may be in place to ensure that information is used in accordance with the above described uses.

The risk of collecting inaccurate information is minimized because CDL holders and the states are expected to have made reasonable efforts to collect accurate data as part of the licensing process. Further, FMCSA audits state licensing agencies on a periodic basis to ensure that CDL records processing meets federal standards. In addition, company owners are required by FMCSA to review driver DMV records annually. Further, the impact of collecting inaccurate information is minimized because individuals who feel they have been wrongly identified as a security threat can seek redress through TSA, allowing for an additional review of the completeness and accuracy of the information.

Section 3.0
Retention

3.1 What is the retention period for the data in the system?

TSA will retain the threat assessment data it receives in accordance with the Transportation Threat Assessment and Credentialing (TTAC) record schedule approved by National Archives and Records Administration (NARA). Records will be retained for one year after an individual no longer holds a CDL, except that records for individuals who are a potential match to a watch list will be retained for seven years, and actual

matches will be retained for 99 years or seven years after the individual is identified to TSA as deceased, whichever is sooner. Records on possible or confirmed watchlist matches, and records associated with the redress process will be retained in accordance with a schedule to be developed within Transportation Sector Network management (TSNM), and will be retained until the schedule is approved by NARA. It is expected that TSNM will seek to retain the records at least seven years for possible matches, and 99 years for confirmed matches.

3.2 Has the retention schedule been approved by the National Archives and Records Administration (NARA)?

Yes. TSA has developed a retention schedule for Transportation Threat Assessment and Credentialing records that was submitted to NARA and was approved on March 8, 2007. Records held within TSNM will be held in accordance with a schedule to be developed.

3.3 Privacy Impact Analysis: Given the purpose of retaining the information, explain why the information is needed for the indicated period.

Information used in this program will be maintained in accordance with a schedule approved by NARA. For legal and operational purposes the retention period is designed to allow TSA to keep threat assessment results for individuals who are cleared for the length of time they retain their CDL plus one year. The schedule provides that threat assessment results on individuals who are initially identified as a potential threat to transportation security, but are subsequently cleared be retained for the length of time they hold their CDLs plus one year, or for seven years after completion of the threat assessment whichever is greater. Finally, the schedule requires TSA to retain records on individuals who are confirmed to be threats to transportation security for 99 years, or seven years after the individual is identified to TSA as deceased, whichever is sooner.

Section 4.0
Internal sharing and disclosure

4.1 With which internal organizations is the information shared?

Individual information may be shared with DHS employees and contractors who have a need for the information in the performance of their duties, including but not

limited to immigration, law enforcement, and intelligence operations. It is expected that information will typically be shared with TSA employees or contractors in the following TSA offices: the Office of Transportation Threat Assessment and Credentialing, the Office of Transportation Sector Network Management, and in the event of a positive match, the Office of Intelligence and the Office of Security Operations. Information might also be shared with the Office of Chief Counsel, Office of Civil Rights and Civil Liberties, Privacy Office, Ombudsman, and Legislative Affairs to respond to complaints or inquires from individuals. All information will be shared in accordance with the provisions of the Privacy Act, 5 U.S.C. § 552a. TSA will share information with the US Citizenship and Immigration Service (USCIS) in the course of performing immigration checks for the STA. While it is not expected that information will otherwise be routinely shared outside of TSA, TSA may need to share information within DHS as outlined in section 4.2, specifically with U.S. Customs and Border Protection (CBP) and Immigration and Customs Enforcement (ICE).

4.2 For each organization, what information is shared and for what purpose?

TSA will share the information with the Office of Transportation Sector Network Management and the Office of Transportation Threat Assessment and Credentialing in order to manage the program and conduct the threat assessments. The information may be shared with the Office of Chief Counsel to review determinations about whether an individual may pose or poses a threat for which TSA should recommend CDL revocation, or to respond to inquiries by individuals. Individuals' identifying information and positive results of comparisons to Federal terrorism, immigration and law enforcement databases will be shared with TSA's Office of Intelligence and Office of Security Operations. In order to respond to complaints or inquiries from individuals, the information may also be shared with the Privacy Office, Ombudsman, Office of Civil Rights and Civil Liberties, and Legislative Affairs. TSA will share information with the USCIS in the course of performing immigration checks for the STA. The information may also be shared within DHS where there is a need to know the information for law enforcement, intelligence, or other official purposes. This information will be shared in accordance with the provisions of the Privacy Act, 5 U.S.C. §552a.

4.3 How is the information transmitted or disclosed?

TSA will transmit this data within DHS via a secure data network, password-protected CD, paper files, facsimile or telephonically to those who need the information to perform their official duties. The method of transmission may vary according to

specific circumstances. The information may also be marked with specific handling requirements and restrictions to further limit distribution.

4.4 Privacy Impact Analysis: Given the internal sharing, discuss what privacy risks were identified and how they were mitigated.

Information is shared within DHS with those individuals who have a need for the information to perform their official duties in accordance with the Privacy Act. Privacy protections include strict access controls, including security credentials, passwords, auditing that tracks access to electronic information, and mandated training for all employees and contractors.

Section 5.0
External sharing and disclosure

5.1 With which external organizations is the information shared?

As an interim measure based on resource constraints, TSA will provide the Terrorist Screening Center with an initial run of the data in order for TSC to perform the STA. In the future, TSA will perform the STA and may share information with the Terrorist Screening Center (TSC) in the event of a need to resolve a potential match as part of the threat assessment. TSA may also share information with Federal, state or local enforcement agencies to facilitate an operational response. TSA may also share information with the Federal Motor Carrier Safety Administration (FMCSA) and the governor of the state that issued the CDL recommending removal of a driver's commercial driving privileges. TSA may share the information it receives with Federal, state, or local law enforcement or intelligence agencies, and state DMV's or licensing agencies in accordance with the routine uses identified in the applicable Privacy Act system of records notice (SORN), DHS/TSA 002, Transportation Security Threat Assessment System (T-STAS). This SORN was last published in the Federal Register on November 8, 2005, and can be found at 70 FR 67731- 67735.

5.2 What information is shared and for what purpose?

TSA will share biographic information with the Terrorist Screening Center (TSC) during the security threat assessment process. When an individual is identified as a security threat, it is expected that individually identifying data and security threat assessment status about the individual will be shared, as needed, with Federal, state, or

local law enforcement and intelligence agencies to communicate threat assessment results and/or to facilitate an operational response.

To facilitate the security threat mitigation process and coordinate CDL status, TSA may share individual information with FMCSA.

5.3 How is the information transmitted or disclosed?

Depending on the recipient and the urgency of the request or disclosure, the information may be disclosed via a secure data network, password-protected CD, paper files, facsimile or telephonically.

5.4 Is a Memorandum of Understanding (MOU), contract, or any agreement in place with any external organizations with whom information is shared, and does the agreement reflect the scope of the information currently shared?

Yes, TSA has entered into an MOU with the TSC governing its threat assessment programs, and a separate agreement regarding the interim access to CDLIS data. In addition, TSA will share information pursuant to routine uses identified in the applicable Privacy Act system of records notice SORN, DHS/TSA 002, Transportation Security Threat Assessment System, or other Privacy Act exceptions. An MOU is in place between TSA and the FMCSA (USDOT) establishing cooperative information-sharing of commercial driver's license information for transportation security purposes.

5.5 How is the shared information secured by the recipient?

TSA shares information in accordance with the Privacy Act. Federal agencies are subject to the safeguarding requirements of the Privacy Act and under the Federal Information Security Management Act (FISMA), Title III of the E-Government Act, (P. L. 107-347).

5.6 What type of training is required for users from agencies outside DHS prior to receiving access to the information?

TSA does not require specific training by outside agencies, however Federal agencies are subject to the Privacy Act, and Federal employees and contractors typically receive mandatory Privacy Act training and Information Security Awareness training.

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

The information shared with FMCSA is largely comprised of data already maintained by FMCSA in commercial driver's license records, thus reducing the risk of producing additional incorrect data. Other risks are mitigated by sharing this information under the applicable provisions of the SORN and the Privacy Act, and by limiting the sharing of this information to those who have a need to know it in the performance of their duties. TSA further mitigates risk by only sharing revocation information after the conclusion of the initial determination and appeal process or in the case of individuals posing an imminent threat to national or transportation security. These individuals are afforded the right to appeal their determination.

Section 6.0 Notice

6.1 Was notice provided to the individual prior to collection of information? If yes, please provide a copy of the notice as an appendix. A notice may include a posted privacy policy, a Privacy Act notice on forms, or a system of records notice published in the Federal Register Notice. If notice was not provided, why not?

The publication of this PIA and of SORN, DHS/TSA 002, Transportation Security Threat Assessment System, serves to provide public notice of the collection, use and maintenance of this information. In the event that an individual is determined to be a security threat and the individual believes that the initial determination of the threat assessment are inaccurate, he or she will be informed by TSA on how to pursue redress. The initial collection of information was performed by the individual States and it is unknown what notices were provided.

6.2 Do individuals have an opportunity and/or right to decline to provide information?

No. Since information is obtained directly from the state licensing agencies without consultation or action by the individual, no opportunity to decline to provide information is provided.

6.3 Do individuals have the right to consent to particular uses of the information, and if so, how does the individual exercise the right?

No. If TSA determines that an individual poses a security threat, all uses of the information by TSA will be consistent with the Privacy Act and SORN DHS/TSA 002, Transportation Security Threat Assessment System identified in paragraph 5.1 above.

6.4 Privacy Impact Analysis: Given the notice provided to individuals above, describe what privacy risks were identified and how you mitigated them.

Since the information TSA uses to conduct the security threat assessment is already collected by each state for their own purposes and will not be collected directly from the CDL holder, there is no notice provided to the individual unless the state chooses to provide notice. The individual information already exists within government databases at the State and Federal level. Privacy risks are mitigated by the notification of initial determination and appeal processes.

Section 7.0
Individual Access, Redress and Correction

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

TSA will obtain all information from driver's licensing records completed by the individual. Individuals may request access to their information by submitting a Freedom of Information Act/Privacy Act (FOIA/PA) request to TSA in writing by mail to the following address:

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

FOIA/PA requests may also be submitted by fax at 571-227-1406 or by filling out the Customer Service Form (URL: http://www.tsa.gov/public/contactus). The FOIA/PA request must contain the following information: full name, address and telephone number, and email address (optional). Please refer to the TSA FOIA web site (http://www.tsa.gov/public). In addition, individuals may amend their records through the redress process as explained in paragraph 7.2 below.

7.2 What are the procedures for correcting erroneous information?

TSA uses the results of the name-based check to make an initial determination as to whether or not the CDL holder poses a security threat to national or transportation security or of terrorism. If TSA determines that the driver does not pose a threat, TSA takes no further action. If TSA determines that a driver may pose a non-imminent threat, TSA mails a letter to the driver at the address listed on the CDL that informs the driver that TSA has initially determined the driver may be a threat to transportation security. This letter provides the reason(s) for that determination and directions for how the driver may submit an appeal. An appeal is the mechanism by which driver can provide objective data to correct or update the records TSA used to make its initial security determination or provide evidence that the driver is not the same person that TSA alleges (mistaken identity). The letter also provides a mechanism for the driver to request an extension of time to gather materials and prepare the appeal. Drivers who believe they have been wrongly identified as posing a security threat must submit the appeal or extension request within 60 days after the date of service of the letter [4] The letter also notifies the driver that if TSA receives no response in the allotted timeframe, the determination will no longer be eligible for appeal, the initial determination will become final, and no additional letter will be mailed.

A driver may submit an appeal by serving TSA with a written answer to the initial determination letter which includes relevant information or court documents to verify the driver's identity and/or correct errors in his or her records. A driver may obtain additional time to respond by appeal by requesting a copy of the documents on which TSA based the Initial Determination or requesting an extension of time. TSA cannot release documents that are classified or otherwise protected by law. TSA will release as much information to the driver as permitted by law to provide for a meaningful appeal.

The appeal process consists of a review of the initial determination, the materials upon which the determination was based, the driver's appeal materials, and any other relevant information or material available to TSA. In cases where TSA's initial determination is based on classified information, the Assistant Secretary or designee reviews the appeal to make a final determination.

Upon review of the appeal, the Assistant Secretary may overturn the initial determination and issue a letter to the driver that withdraws the initial determination. Conversely, if the Assistant Secretary upholds the initial determination (i.e., denies the applicant's appeal), TSA issues a letter to the driver declaring that the determination is final. For purposes of judicial review, this final determination constitutes a final TSA order. TSA may also notify the Administrator of FMCSA and the Governor (or his/her

[4] The date of service is date 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.

designee) of the licensing State of the FDTA. TSA may recommend that the Governor or the FMCSA revoke the driver's CDL.

Depending on the nature of the information disclosed during the name-based check, TSA may determine that a driver poses an imminent threat to national or transportation security or of terrorism. In this case, TSA notifies the FMCSA and the Governor (or his/her designee) of the licensing State of TSA's determination and the information on which it is based. TSA may recommend that the Governor or the FMCSA revoke the driver's CDL. Also, TSA mails a letter to the driver at the address listed on the CDL that informs the driver TSA has initially determined the driver may be an imminent threat to transportation security. This letter provides the reason(s) for that determination and directions for how the driver may submit an appeal. Drivers who believe they have been wrongly identified as posing a security threat must submit the appeal or extension request within 60 days after the date of service of the letter. The letter also notifies the driver that if TSA receives no response in the allotted timeframe, the determination will no longer be eligible for appeal, the initial determination will become final, and no additional letter will be mailed.

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

The initial determination letter sent to the individual will contain the procedures for submitting appeals. Individuals may also seek correction of underlying records through the agencies that maintain those records. In addition to the redress process, the individual may also request correction of his or her records pursuant to the Privacy Act.

7.4 If no redress is provided, are alternatives are available?

N/A. A redress process, as described in section 7.2 above, is provided for individuals who believe that they have been wrongfully identified as a threat.

7.5 Privacy Impact Analysis: Given the access and other procedural rights provided for in the Privacy Act of 1974, explain the procedural rights that are provided and, if access, correction and redress rights are not provided please explain why not.

The risk identified with access is that incorrect information might be associated with an individual. In order to mitigate this risk, a redress process has been developed that provides notice to the individual of the determination and how to access and/or correct the information.

Section 8.0
Technical Access and Security

8.1 Which user group(s) will have access to the system?

In order to manage, upgrade and utilize the TSA system, system administrators, security administrators, IT specialists, vetting operators, analysts and other persons may have a need to access the TSA system or the information in the system in the performance of their duties. Role-based access controls are employed to limit the access of information by different users based on the need to know. TSA also employs processes to enforce separation of duties to prevent unauthorized disclosure or modification of information. No unauthorized users are permitted access to system resources. Strict adherence to access control policies is automatically enforced by the TSA system in coordination with and through oversight by TSA security officers.

8.2 Will contractors to DHS have access to the system?

Contractors who are hired to perform many of the IT maintenance and security monitoring tasks have access to the system in order to perform their official duties. Strict adherence to access control policies is automatically enforced by the system in coordination with and through oversight by TSA IT Security Officers. All contractors performing this work are subjected to requirements for suitability and a background investigation as required by TSA Management Directive 1400.3, TSA Information Security Policy.

8.3 Does the system use "roles" to assign privileges to users of the system?

Yes. Role-based access controls are used for controlling access to the system using the policy of Least Privilege, which states that the system will enforce the most restrictive set of rights/privileges or access needed by users based on their roles.

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

Limited system access will be provided for purposes of conducting these security threat assessments. Generally, the system is secured against unauthorized use by a layered, defense-in-depth security approach involving procedural and information security safeguards.

All TSA and DHS employees and assigned contractor staff receive DHS-mandatory privacy training on the use and disclosure of personal data. They also

receive appropriate security training and have any necessary background investigations and/or security clearances for access to sensitive information or secured facilities based on TSA security policies and procedures.

All government and contractor personnel are vetted and approved access to the facility where the system is housed, issued picture badges with integrated proximity devices imbedded. A rules of behavior document provides an overall guidance of how employees are to protect their physical and technical environment and the data that is handled and processed. All new employees are required to read and sign a copy of a rule of behavior document prior to getting access to any IT system.

8.5 How are the actual assignments of roles and rules verified according to established security and auditing procedures?

Employees or contractors are assigned roles for accessing the system based on their function. TSA ensures personnel accessing the system have security training commensurate with their duties and responsibilities. All personnel are trained through TSA's Security and Awareness Training Program when they join the organization and periodically thereafter. The status of personnel who have completed the training is reported to TSA on a monthly basis. The Facility Security Officer ensures compliance with policy and manages the activation or deactivation of accounts and privileges as required or when expired.

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

The system is continuously monitored to audit compliance with policy. Weekly logs are reviewed to ensure that no unauthorized access has taken place. The TSA IT Security Office reviews all IT systems annually for IT security policy compliance and technical vulnerability.

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

All government and contractor personnel are required to complete on-line TSA Privacy Training. The TSA Privacy Office monitors compliance with this requirement monthly. In addition, security training is provided regularly, which helps to raise the level of awareness for protecting personal information being processed. All IT security training is reported as required in the Federal Information Security Management Act of 2002, Pub.L.107-347 (FISMA).

8.8 Is the data secured in accordance with FISMA requirements? If yes, when was Certification & Accreditation last completed?

Yes. Information in TSA's record systems is safeguarded in accordance with FISMA, which establishes government-wide computer security and training standards for all persons associated with the management and operation of Federal computer systems. All systems are operating on the authority of the Designated Accrediting Authority (DAA). Certification and Accreditation was received on September 1, 2005.

8.9 Privacy Impact Analysis: Given access and security controls, what privacy risks were identified and describe how they were mitigated.

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

Section 9.0 Technology

9.1 Was the system built from the ground up or purchased and installed?

The TSA system is primarily built from Commercial Off-The-Shelf (COTS) products. TSA system components include COTS hardware and operating systems. This system was provided to TSA from the Department of Transportation upon TSA stand-up.

9.2 Describe how data integrity, privacy, and security were analyzed as part of the decisions made for your system.

TSA collects only those data elements necessary to allow TSA to complete its tasks. Additional information is only requested as needed and in the vast majority of cases, a limited initial set of information will be sufficient to resolve adjudication questions related to the security threat assessment.

9.3 What design choices were made to enhance privacy?

In order to support privacy protections, TSA has limited its data collection to specific elements necessary for security vetting. TSA has developed an information technology infrastructure that will protect against inadvertent use of personally identifying information not required by the government. Access to data collected for this program will be strictly controlled; only TSA employees and contractors with proper access controls will have permission to use and view this information. TSA will not transmit or otherwise share this information with entities outside of DHS that are not listed in the routine uses in Privacy Act System of Records Notice DHS/TSA 002, which is described above. Additionally, the record system will include a real time audit function to track access to electronic information, and any infractions of information security rules will be addressed appropriately. TSA will adhere to strict incident response plans. All TSA and assigned contractor staff receive TSA-mandated privacy training on the use and disclosure of personal data. The procedures and policies in place are intended to ensure that no unauthorized access to records occurs and that operational safeguards are firmly in place to prevent system abuses.

9.4 Privacy Impact Analysis

These conscious design choices will limit access to the personal information, thereby mitigating any possible privacy risks associated with this program. Information received from the applicant is limited to data needed to operate the program, including facilitating adjudication to resolve potential matches without the delay and cost associated with requesting additional information from the applicant.

Conclusion

TSA is performing these threat assessments for the limited purpose of assessing the risks to transportation security associated with permitting covered individuals to hold CDLs. Privacy impacts associated with this have been minimized by collecting information already provided to government and employing appropriate technical and operational safeguards and requirements. If TSA makes any changes to this program or the data elements needed for conducting the relevant security threat assessments or other checks on individuals, those changes will be reflected in an amended version of this PIA.

Approval Signature Page

Original signed and on file with the DHS Privacy Office

Hugo Teufel III
Chief Privacy Officer
Department of Homeland Security